PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-308840
(43)Date of publication of application : 02.11.2001

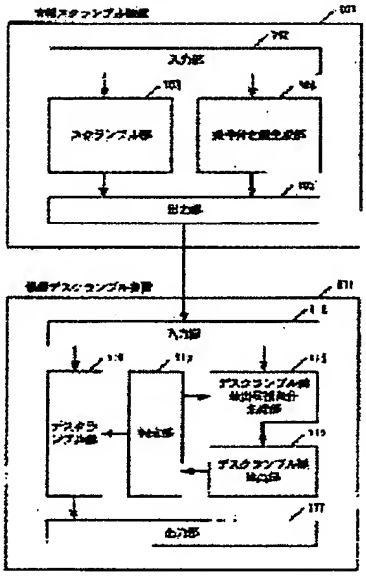
(51)Int.Cl. H04L 9/08
G10L 11/00
G10L 19/00
H04N 7/16

(21)Application number : 2000-116057
(22)Date of filing : 18.04.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : OKADA YASUNORI

(54) KEY MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To construct such a key management system where an information originator side can control the conditions for disclosing information contents to be provided to users.
SOLUTION: An information scrambling device 101 generates a conditional key, by using a descrambling key at the time of descrambling scrambled information and prescribed conditions for descrambling the scrambled information and outputs the scrambled information and the conditional key. An information descrambling device 111 extracts the descrambling key from the conditional key, descrambles the scrambled information with the descrambling key and outputs the scrambled information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－308840
（P2001－308840A）
(43)公開日　平成13年11月２日(2001.11.2)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｎ　7/16	Ｃ	５Ｃ０６４
Ｇ１０Ｌ　11/00		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
19/00		Ｇ１０Ｌ　9/00	Ｅ	
Ｈ０４Ｎ　7/16			Ｎ	

審査請求　未請求　請求項の数38　ＯＬ　（全 32 頁）

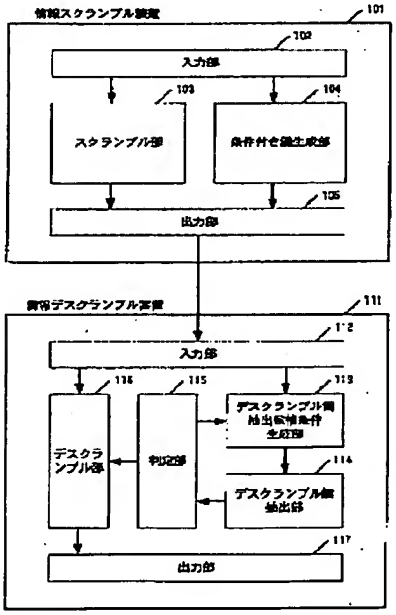
(21)出願番号　特願2000－116057(P2000－116057)
(22)出願日　平成12年４月18日(2000.4.18)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　岡田　義典
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5C064 CA14 CB01 CC01 CC04
5J104 AA01 AA16 EA01 EA06 EA23 NA02 PA07

(54)【発明の名称】　鍵管理システム

(57)【要約】
【課題】　利用者に提供する情報の内容を公開するための条件を情報の発信者側で制御できるような鍵管理システムを構築することを目的とする。
【解決手段】　情報スクランブル装置１０１は、スクランブルした情報をデスクランブルする時のデスクランブル鍵と、スクランブルした情報をデスクランブルするための所定の条件とを用いて条件付き鍵を生成し、スクランブルした情報及び条件付き鍵を出力する。情報デスクランブル装置１１１は、条件付き鍵からデスクランブル鍵を抽出し、スクランブルされた情報をデスクランブル鍵によりデスクランブルし、出力する。



1

【特許請求の範囲】

【請求項1】 画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を出力する情報スクランブル装置と、前記スクランブル情報を入力し前記スクランブル情報をデスクランブルした前記情報を出力する情報デスクランブル装置とからなる鍵管理システムであって、

前記情報スクランブル装置は、

前記情報と、前記情報のスクランブルを行うスクランブル鍵と、

スクランブルされた前記情報のデスクランブルを行うデスクランブル鍵とを入力する入力手段と、

前記情報を前記スクランブル鍵によりスクランブルしたスクランブル情報を生成するスクランブル手段と、

前記デスクランブル鍵と、前記スクランブル情報をデスクランブルするための所定の条件とを用いて、前記スクランブル情報をデスクランブルするための条件付き鍵を生成する条件付き鍵生成手段と、

前記スクランブル情報と前記条件付き鍵とを出力する出力手段とを有し、

前記情報デスクランブル装置は、

前記スクランブル情報と、前記条件付き鍵とを入力する入力手段と、

前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成手段と、

前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出手段と、

前記デスクランブル鍵抽出手段により前記デスクランブル鍵が抽出されたか否かを判定する判定手段と、

前記判定手段により前記デスクランブル鍵が抽出されたと判定された時に、抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記情報を抽出するデスクランブル手段と、

デスクランブルされた前記情報を出力する出力手段とを有することを特徴とする鍵管理システム。

【請求項2】 前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、

前記デスクランブル鍵抽出候補条件生成手段は、現在日時を前記デスクランブル鍵抽出候補条件として生成し、

前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件生成手段で生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出することを特徴とする請求項1記載の鍵管理システム。

【請求項3】 前記情報スクランブル装置は、前記情報を複数の前記情報デスクランブル装置側に対して出力するにあたり、

2

前記情報デスクランブル装置に対応して、前記デスクランブル鍵と、前記条件付き鍵とのいずれかを選択する鍵選択手段を有し、

前記出力手段は、前記鍵選択手段で選択された前記デスクランブル鍵と前記条件付き鍵とのいずれかを出力し、

前記情報デスクランブル装置はさらに、

入力手段が前記デスクランブル鍵を入力した場合に前記デスクランブル鍵の前記デスクランブル手段への出力を行う切り換え手段を有し、

前記デスクランブル手段は、前記切り換え手段から入力した前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルすることを特徴とする請求項1または2記載の鍵管理システム。

【請求項4】 画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む第1の情報及び第2の情報を入力し、前記第1の情報をスクランブルしたスクランブル情報と、前記第2の情報とを出力する情報スクランブル装置と、前記スクランブル情報と前記第2の情報とを入力し、前記スクランブル情報をデスクランブルして出力する情報デスクランブル装置とからなる鍵管理システムであって、

前記情報スクランブル装置は、

前記第1の情報と、前記第2の情報と、前記第1の情報のスクランブルを行うスクランブル鍵と、スクランブルされた前記第1の情報のデスクランブルを行うデスクランブル鍵とを入力する入力手段と、

前記第1の情報を前記スクランブル鍵によりスクランブルしたスクランブル情報を生成するスクランブル手段と、

前記デスクランブル鍵と、前記スクランブル情報をデスクランブルするための所定の条件とを用いて、前記スクランブル情報をデスクランブルするための条件付き鍵を生成する条件付き鍵生成手段と、

前記第2の情報への前記デスクランブル鍵の多重と、前記スクランブル情報への前記条件付き鍵の多重とをそれぞれ行う多重手段と、

前記多重手段により多重された前記スクランブル情報と、前記多重手段により多重された前記第2の情報とを出力する出力手段とを有し、

前記情報デスクランブル装置は、

前記スクランブル情報または前記第2の情報を入力する入力手段と、

前記入力手段に前記スクランブル情報が入力された場合に、前記スクランブル情報と前記スクランブル情報に多重された前記条件付き鍵との分離と、前記入力手段に前記第2の情報が入力された場合に、前記第2の情報と前記第2の情報に多重された前記デスクランブル鍵との分離とを行う分離手段と、

前記入力手段に前記スクランブル情報が入力された場合

に、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成手段と、

前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出手段と、

前記デスクランブル鍵抽出手段により前記デスクランブル鍵が抽出されたか否かを判定する判定手段と、

前記判定手段により前記デスクランブル鍵が抽出されたと判定された時に、前記デスクランブル鍵抽出手段により抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記第１の情報の抽出と、前記分離手段により前記デスクランブル鍵が分離された場合には、前記入力手段に前記スクランブル情報が入力された時に、前記分離手段により前記第２の情報から分離された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記第１の情報の抽出とをそれぞれ行うデスクランブル手段とを有することを特徴とする鍵管理システム。

【請求項５】　前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、

前記デスクランブル鍵抽出候補条件生成手段は、現在日時を前記デスクランブル鍵抽出候補条件として生成し、

前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件生成手段で生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出し、

前記デスクランブル手段は、前記入力手段に前記スクランブル情報が入力された時に、抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルすることを特徴とする請求項４記載の鍵管理システム。

【請求項６】　前記デスクランブル装置はさらに、前記入力手段により入力した前記スクランブル情報及び前記第２の情報を記録する記録手段を有し、

前記分離手段は、前記記録手段により記録された前記第２の情報を読み出し、前記第２の情報と前記第２の情報に多重された前記デスクランブル鍵を分離し、

前記デスクランブル手段は、前記記録手段により記録された前記スクランブル情報を読み出し、前記分離手段により前記第２の情報から分離された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルすることを特徴とする請求項４記載の鍵管理システム。

【請求項７】　前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、

前記多重手段は、前記第２の情報に前記デスクランブル鍵の代わりに前記スクランブル情報の公開許可日時を表す情報を多重し、

前記情報デスクランブル装置において、

前記分離手段は、前記記録手段により記録された前記第２の情報を読み出し、前記第２の情報と、前記第２の情報に多重された前記公開許可日時を分離し、

前記デスクランブル鍵抽出手段は、分離された前記公開許可日時を用いて、前記分離手段により分離した前記条件付き鍵から前記デスクランブル鍵を抽出し、

前記デスクランブル手段は、前記記録手段により記録された前記スクランブル情報を読み出し、抽出された前記デスクランブル鍵を用いて、前記スクランブル情報をデスクランブルすることを特徴とする請求項６記載の鍵管理システム。

【請求項８】　前記情報スクランブル装置はさらに、前記第１の情報と前記第２の情報とを符号化する符号化手段と、

符号化する前の前記第２の情報の一部をスクランブル鍵として生成するスクランブル鍵生成手段とを有し、

前記スクランブル手段は、前記スクランブル鍵生成手段で生成されたスクランブル鍵により符号化された前記第１の情報をスクランブルし前記スクランブル情報を生成し、

前記出力手段は、符号化した前記第２の情報と、前記スクランブル情報とを出力し、

前記情報デスクランブル装置はさらに、

前記デスクランブル手段により抽出された前記第１の情報と、前記第２の情報とを復号化する復号化手段と、

復号化された前記第２の情報の一部をデスクランブル鍵として分離するデスクランブル鍵分離手段とを有し、

前記デスクランブル手段は、前記デスクランブル鍵分離手段により分離した前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルして前記第１の情報を抽出し、

前記復号化手段は、抽出された前記第１の情報を復号化することを特長とする請求項６記載の鍵管理システム。

【請求項９】　前記第１の情報は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む番組であり、

前記第２の情報は、画像と音声と前記画像及び前記音声以外のデータの単独又は組み合わせを含む広告であることを特徴とする請求項４～８いずれかに記載の鍵管理システム。

【請求項１０】　前記条件付き鍵生成手段は、前記スクランブル情報をデスクランブルする所定の条件を鍵として、前記デスクランブル鍵をスクランブルし前記条件付き鍵を生成し、

前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件を鍵として、前記条件付き鍵をデスクランブルすることを特長とする請求項１～９記載の鍵管理システム。

【請求項１１】 前記情報スクランブル装置は、前記スクランブル情報を複数の前記情報デスクランブル装置に対して出力するにあたり、
前記条件付き鍵生成手段は、前記情報デスクランブル装置毎にそれぞれ異なる条件で前記スクランブル情報をデスクランブルするための前記条件付き鍵をそれぞれ生成することを特長とする請求項１～１０いずれかに記載の鍵管理システム。

【請求項１２】 前記条件付き鍵生成手段は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせで構成される要素毎にそれぞれ異なる条件で前記スクランブル情報をデスクランブルするための前記条件付き鍵をそれぞれ生成することを特長とする請求項１～１０いずれかに記載の鍵管理システム。

【請求項１３】 画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を出力する情報スクランブル装置であって、
前記情報と、前記情報のスクランブルを行うスクランブル鍵と、
スクランブルされた前記情報のデスクランブルを行うデスクランブル鍵とを入力する入力手段と、
前記情報を前記スクランブル鍵によりスクランブルしたスクランブル情報を生成するスクランブル手段と、
前記デスクランブル鍵と、前記スクランブル情報をデスクランブルするための所定の条件とを用いて、前記スクランブル情報をデスクランブルするための条件付き鍵を生成する条件付き鍵生成手段と、
前記スクランブル情報と前記条件付き鍵とを出力する出力手段とを有することを特徴とする情報スクランブル装置。

【請求項１４】 前記スクランブル情報をデスクランブルするための所定の条件が前記スクランブル情報の公開許可日時であることを特徴とする請求項１３記載の情報スクランブル装置。

【請求項１５】 前記情報スクランブル装置は、前記情報を複数の前記情報デスクランブル装置側に対して出力するにあたり、
前記情報デスクランブル装置に対応して、前記デスクランブル鍵と、前記条件付き鍵とのいずれかを選択する鍵選択手段を有し、
前記出力手段は、前記鍵選択手段で選択された前記デスクランブル鍵と前記条件付き鍵とのいずれかを出力すること特徴とする請求項１３～１４いずれかに記載の情報スクランブル装置。

【請求項１６】 画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む第１の情報及び第２の情報を入力し、前記第１の情報をスクランブルしたスクランブル情報と、前記第２の情報とを出力する情報スクランブル装置であって、

前記第１の情報と、前記第２の情報と、前記第１の情報のスクランブルを行うスクランブル鍵と、スクランブルされた前記第１の情報のデスクランブルを行うデスクランブル鍵とを入力する入力手段と、
前記第１の情報を前記スクランブル鍵によりスクランブルしたスクランブル情報を生成するスクランブル手段と、
前記デスクランブル鍵と、前記スクランブル情報をデスクランブルするための所定の条件とを用いて、前記スクランブル情報をデスクランブルするための条件付き鍵を生成する条件付き鍵生成手段と、
前記第２の情報への前記デスクランブル鍵の多重と、前記スクランブル情報への前記条件付き鍵の多重とをそれぞれ行う多重手段と、
前記多重手段により多重された前記スクランブル情報と、前記多重手段により多重された前記第２の情報とを出力する出力手段とを有する情報スクランブル装置。

【請求項１７】 前記スクランブル情報をデスクランブルするための所定の条件が前記スクランブル情報の公開許可日時であることを特徴とする請求項１６記載の情報スクランブル装置。

【請求項１８】 前記多重手段は、前記第２の情報に前記デスクランブル鍵の代わりに前記スクランブル情報の公開許可日時を表す情報を多重することを特徴とする請求項１７記載の情報スクランブル装置。

【請求項１９】 前記情報スクランブル装置はさらに、前記第１の情報と前記第２の情報とを符号化する符号化手段と、符号化する前の前記第２の情報の一部をスクランブル鍵として生成するスクランブル鍵生成手段とを有し、
前記スクランブル手段は、前記スクランブル鍵生成手段で生成されたスクランブル鍵により符号化された前記第１の情報をスクランブルし前記スクランブル情報を生成し、
前記出力手段は、符号化した前記第２の情報と、前記スクランブル情報とを出力することを特徴とする請求項１６～１８いずれかに記載の情報スクランブル装置。

【請求項２０】 前記第１の情報は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む番組であり、
前記第２の情報は、画像と音声と前記画像及び前記音声以外のデータの単独又は組み合わせを含む広告であることを特徴とする請求項１６～１９いずれかに記載の情報スクランブル装置。

【請求項２１】 前記条件付き鍵生成手段は、前記条件付き鍵から前記スクランブル鍵をデスクランブル可能とする所定の条件を鍵として、前記スクランブル鍵をスクランブルし前記条件付き鍵を生成することを特徴とする請求項１３～２０記載の情報スクランブル装置。

【請求項２２】 前記情報スクランブル装置は、前記ス

7

クランブル情報を複数の前記情報デスクランブル装置に対して出力するにあたり、
前記条件付き鍵生成手段は、前記情報デスクランブル装置毎にそれぞれ異なる条件で前記スクランブル情報をデスクランブルするための前記条件付き鍵をそれぞれ生成することを特徴とする請求項１３～２１いずれかに記載の情報スクランブル装置。

【請求項２３】　前記条件付き鍵生成手段は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせで構成される要素毎にそれぞれ異なる条件で前記スクランブル情報をデスクランブルするための前記条件付き鍵をそれぞれ生成することを特徴とする請求項１３～２１いずれかに記載の情報スクランブル装置。

【請求項２４】　画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む情報に対して、前記情報をスクランブルしたスクランブル情報と、前記スクランブル情報をデスクランブルするデスクランブル鍵を、所定の条件においてのみ抽出する条件付き鍵とを入力し、前記スクランブル情報をデスクランブルし出力する情報デスクランブル装置であって、
前記スクランブル情報と、前記条件付き鍵とを入力する入力手段と、
前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成手段と、
前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出手段と、
前記デスクランブル鍵抽出手段により前記デスクランブル鍵が抽出されたか否かを判定する判定手段と、
前記判定手段により前記デスクランブル鍵が抽出されたと判定された時に、抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記情報を抽出するデスクランブル手段と、
デスクランブルされた前記情報を出力する出力手段とを有することを特徴とする情報デスクランブル装置。

【請求項２５】　前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、
前記デスクランブル鍵抽出候補条件生成手段は、現在日時を前記デスクランブル鍵抽出候補条件として生成し、
前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件生成手段で生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出することを特徴とする請求項２４記載の情報デスクランブル装置。

【請求項２６】　前記入力手段は、前記条件付き鍵または前記スクランブル鍵の何れかを入力し、

8

前記情報デスクランブル装置はさらに、
入力手段が前記デスクランブル鍵を入力した場合に前記デスクランブル鍵の前記デスクランブル手段への出力を行う切り換え手段を有し、
前記デスクランブル手段が、前記切り換え手段により入力した前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルすることを特徴とする請求項２５または２６いずれかに記載の情報デスクランブル装置。

【請求項２７】　画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む第１の情報及び第２の情報に対して、前記第１の情報をスクランブルし、スクランブルした前記第１の情報をデスクランブルするデスクランブル鍵を、所定の条件においてのみ抽出する条件付き鍵を多重したスクランブル情報または第１の情報をデスクランブルするデスクランブル鍵を多重した前記第２の情報を入力し、前記スクランブル情報をデスクランブルし出力する情報デスクランブル装置であって、
前記スクランブル情報または前記第２の情報を入力する入力手段と、
前記入力手段に前記スクランブル情報が入力された場合に、前記スクランブル情報と前記スクランブル情報に多重された前記条件付き鍵との分離と、前記入力手段に前記第２の情報が入力された場合に、前記第２の情報と前記第２の情報に多重された前記デスクランブル鍵との分離とを行う分離手段と、
前記入力手段に前記スクランブル情報が入力された場合に、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成手段と、
前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出手段と、
前記デスクランブル鍵抽出手段により前記デスクランブル鍵が抽出されたか否かを判定する判定手段と、
前記判定手段により前記デスクランブル鍵が抽出されたと判定された時に、前記デスクランブル鍵抽出手段により抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記第１の情報の抽出と、前記分離手段により前記デスクランブル鍵が分離されている場合には、前記入力手段に前記スクランブル情報が入力された時に、前記分離手段により前記第２の情報から分離された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記第１の情報の抽出とを行うデスクランブル手段とを有することを特徴とする情報デスクランブル装置。

【請求項２８】　前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、

前記デスクランブル鍵抽出候補条件生成手段は、現在日時を前記デスクランブル鍵抽出候補条件として生成し、

前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件生成手段で生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出し、

前記デスクランブル手段は、前記入力手段に前記スクランブル情報が入力された時に、抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルすることを特徴とする請求項２７記載の情報デスクランブル装置。

【請求項２９】　前記デスクランブル装置はさらに、前記入力手段により入力した前記スクランブル情報及び前記第２の情報を記録する記録手段を有し、

前記分離手段は、前記記録手段により記録された前記第２の情報を読み出し、前記第２の情報と前記第２の情報に多重された前記デスクランブル鍵を分離し、

前記デスクランブル手段は、前記記録手段により記録された前記スクランブル情報を読み出し、前記分離手段により前記第２の情報から分離された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルすることを特徴とする請求項２７記載の情報デスクランブル装置。

【請求項３０】　前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、

前記第２の情報は、前記デスクランブル鍵の代わりに前記スクランブル情報の公開許可日時を表す情報が多重されており、

前記分離手段は、前記記録手段により記録された前記第２の情報を読み出し、前記第２の情報と、前記第２の情報に多重された前記公開許可日時を分離し、

前記デスクランブル鍵抽出手段は、分離された前記公開許可日時を用いて、前記分離手段により分離した前記条件付き鍵から前記デスクランブル鍵を抽出し、

前記デスクランブル手段は、前記記録手段により記録された前記スクランブル情報を読み出し、抽出された前記デスクランブル鍵を用いて、前記スクランブル情報をデスクランブルすることを特徴とする請求項２９記載の情報デスクランブル装置。

【請求項３１】　前記入力手段は、前記第２の情報の一部をスクランブル鍵として、符号化された前記第１の情報をスクランブルした前記スクランブル情報と、符号化された前記第２の情報とを入力し、

前記情報デスクランブル装置はさらに、

前記デスクランブル手段により抽出された前記第１の情報と、前記第２の情報とを復号化する復号化手段と、

復号化された前記第２の情報の一部をデスクランブル鍵として分離するデスクランブル鍵分離手段とを有し、

前記デスクランブル手段は、前記デスクランブル鍵分離手段により分離した前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルして前記第１の情報を抽出し、

前記復号化手段は、抽出された前記第１の情報を復号化することを特徴とする請求項２９記載の情報デスクランブル装置。

【請求項３２】　前記第１の情報は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む番組であり、

前記第２の情報は、画像と音声と前記画像及び前記音声以外のデータの単独又は組み合わせを含む広告であることを特徴とする請求項２７～３１いずれかに記載の情報デスクランブル装置。

【請求項３３】　前記条件付き鍵は、前記スクランブル情報をデスクランブルするための所定の条件を鍵として、前記デスクランブル鍵をスクランブルし生成されており、

前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件を鍵として、前記条件付き鍵をデスクランブルすることを特徴とする請求項２４～３２いずれかに記載の情報デスクランブル装置。

【請求項３４】　情報をスクランブル化したスクランブル情報を入力し、前記スクランブル情報をデスクランブルして出力するための情報デスクランブル装置が、読み取り実行可能なプログラムを記録した記録媒体であって、

前記記録媒体は、前記スクランブル情報をデスクランブルする所定の条件を用いて生成された条件付き鍵を入力する入力ステップと、

前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成ステップと、

前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出ステップと、

前記デスクランブル鍵抽出ステップにより前記デスクランブル鍵が抽出されたか否かを判定する判定ステップと、

前記判定ステップにより前記デスクランブル鍵が抽出されたと判定された時に、抽出された前記デスクランブル鍵を出力する出力ステップとを前記情報デスクランブル装置に実行させるプログラムを含むことを特徴とする記録媒体。

【請求項３５】　前記前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、

前記デスクランブル鍵抽出候補条件生成ステップは、現在日時を前記デスクランブル鍵抽出候補条件として生成し、

前記デスクランブル鍵抽出ステップは、前記デスクランブル鍵抽出候補条件生成ステップで生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出することを特徴とする請求項３４記載の記録媒体。

【請求項３６】　前記入力ステップは、前記条件付き鍵または前記デスクランブル鍵の何れかを入力し、

前記入力ステップにより前記デスクランブル鍵が入力された場合は、前記出力ステップは、前記入力ステップで入力された前記スクランブル鍵をそのまま出力することを特徴とする請求項３４または３５に記載の記録媒体。

【請求項３７】　前記入力ステップが、前記スクランブル情報の公開許可日時を表す情報を入力した場合は、前記デスクランブル鍵抽出ステップは、前記公開許可日時を用いて、前記条件付き鍵から前記デスクランブル鍵を抽出することを特徴とする請求項３４～３６のいずれかに記載の記録媒体。

【請求項３８】　前記入力ステップが入力する前記条件付き鍵は、前記スクランブル情報をデスクランブルするための所定の条件を鍵として、前記デスクランブル鍵をスクランブルし生成されており、

前記デスクランブル鍵抽出ステップは、前記デスクランブル鍵抽出候補条件を鍵として、前記条件付き鍵をデスクランブルすることを特徴とする請求項３４～３７のいずれかに記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、スクランブル化された情報をデスクランブルするデスクランブル鍵を管理するための鍵管理システムに関するものである。特に、情報を受け取った利用者に対して情報を公開する条件を情報の発信者側で制御するシステムに関するものである。

【０００２】

【従来の技術】近年、インターネットなどの通信媒体を用いて複数の端末に対して必要な情報を提供するサービス（以下「配信サービス」と記述）が行われている。

【０００３】また、不特定多数の端末に対して同一の情報を提供する放送サービスについては、衛星放送や地上波放送が行われている。放送される番組としては、無料で放送される番組と視聴者が料金を支払って視聴する有料番組とがある。有料番組の形態としては番組のスポンサーが番組制作費用などを負担する代わりに番組の途中などにスポンサーの広告（ＣＭ）を挿入し、その結果として低料金で視聴者に提供するというものも考えられる。

【０００４】有料番組については、視聴者が放送事業者と受信契約を行うことにより、各視聴者毎に固有の鍵情報（マスタ鍵）が与えられ、このマスタ鍵によって受信資格が判定され、放送波に埋め込まれたスクランブル鍵

を再生し、スクランブルされた番組をデスクランブルして視聴することが出来る。

【０００５】近年衛星放送や地上波放送のディジタル化が進められているが、将来的には番組をスクランブルされた状態でディジタルＶＴＲなどの録画装置に記録し、受信契約者は放送時刻以外の好きな時間帯に自由に視聴することが出来る（タイムシフト視聴）ようになることが考えられる。

【０００６】ところで、配信サービスにおいて情報提供者から端末に対して提供される情報の中にはある時期までは情報の内容を秘密にしておく必要があるが、その時期以降では内容を公開しても良いという性質のものがある。

【０００７】例えば、通信販売の商品リストの場合、公開日までは他の店に知られたくない、等の理由で内容を秘密にし、かつ公開日には利用者に対してリストを同時に公開したい場合がある。また、電子音楽配信のようなサービスでは、販売促進及び宣伝活動の一環として特定の期間だけ内容を公開出来る（音楽が聴ける）ような仕組みがあることが望まれる。

【０００８】このように、情報提供者側が指定した時期に提供した情報の内容を利用者に対して同時に公開出来るように制御するために、特開平１１－２７２５２では次のような方式が提案されている。その動作について図２５を用いて説明する。

【０００９】図中、情報スクランブル装置２５１０は利用者に対して提供する情報をスクランブル化した上で送信する。情報デスクランブル装置２５２０は情報スクランブル装置２５１０が送信した情報を受信し、スクランブル化された情報をデスクランブルして元の情報に復元する。鍵管理装置２５００は情報スクランブル装置２５１０がスクランブルするスクランブル鍵と情報デスクランブル装置２５２０が使用するデスクランブル鍵とを管理する。ネットワーク２５３０は情報スクランブル装置２５１０と情報デスクランブル装置２５２０と鍵管理装置２５００とを結合し、情報の伝送媒体の役目を果たす。

【００１０】情報スクランブル装置２５１０は鍵管理装置２５００が管理しているスクランブル化した情報のデスクランブル鍵とその公開日時との対応関係を示す管理テーブル２５０１を参照して送信情報が要求した日時に対応したデスクランブル鍵と対のスクランブル鍵を検索し、そのスクランブル鍵を用いて情報をスクランブル化する。スクランブル化した情報に公開日時を付与して情報デスクランブル装置２５２０に送信する。情報受信装置２５２０では、現在日時が受け取った情報に付与されたＨ時になったときに対応するデスクランブル鍵を鍵管理装置２５００からネットワーク２５３０を通じて取得し、取得したデスクランブル鍵を用いてスクランブル化された情報をデスクランブルする。

【００１１】一方、放送サービスにおいては、多くのスポンサーを獲得し、より低価格で番組を提供することが望まれる。そのためには、ＣＭによる宣伝効果を上げ、スポンサーの参入を促進することが必要である。

【００１２】特開平１０－１６４５５０では視聴者が番組中に挿入されたＣＭを見ることを保証する方式が提案されている。以下、図２６を参照して方式の内容を説明する。

【００１３】番組２６０７、２６０８及び２６０９をスクランブルする。それぞれの番組をデスクランブルするために使用するデスクランブル鍵２６０４、２６０５及び２６０６をそれぞれＣＭ２６０１、２６０２及び２６０３に多重して放送する。視聴者は番組２６０７に先立って放送されたＣＭ２６０１を視聴し、ＣＭ２６０１に多重されたデスクランブル鍵２６０４を取得することによって番組２６０７をデスクランブルして視聴することが出来る。

【００１４】上記方式により、視聴者がＣＭを視聴するという条件を満たすことによって情報（番組）を公開するように放送局側で制御することが出来る。

【００１５】

【発明が解決しようとする課題】しかしながら、特開平１１－２７２５２の方式では送信する情報に公開日時情報を付与しなければならないという課題がある。また、公開日時になったらネットワークまたは無線などの伝送媒体を通してデスクランブル鍵を取得しなければならないという課題がある。

【００１６】また、特開平１０－１６４５５０の方式では番組チャネルで放送されるＣＭを専門に放送するＣＭ専用チャネルを設け、番組の途中から視聴を開始する場合は一旦ＣＭチャネルに移動し、ＣＭを視聴してデスクランブル鍵を取得してから番組チャネルに戻って番組を視聴する。図２６のように１０時から始まる番組を視聴するために１０時に視聴を開始した場合、ＣＭ２６０１が仮に３分のＣＭであったとすると、画面表示は図２６に示したように、１０時から１０時３分まではＣＭ２６０１が表示され、１０時３分からは番組２６０７が表示される。このように、視聴者は１０時から視聴開始したにも関わらず１０時３分からしか番組を視聴することが出来ない。

【００１７】また、ＣＭ専用チャネルで放送しているＣＭの途中で視聴開始した場合、ＣＭを視聴してデスクランブル鍵が取得できないため、番組が視聴出来ないという課題がある。

【００１８】本発明はこれらの課題を解決し、配信サービスや放送サービスにおいて情報を受信した利用者に対して情報を公開する条件を情報の発信者側で制御出来る鍵管理システムを提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明は上記課題を解決

するために、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を出力する情報スクランブル装置と、前記スクランブル情報を入力し前記スクランブル情報をデスクランブルした前記情報を出力する情報デスクランブル装置とからなる鍵管理システムであって．前記情報スクランブル装置は、前記情報と、前記情報のスクランブルを行うスクランブル鍵と、スクランブルされた前記情報のデスクランブルを行うデスクランブル鍵とを入力する入力手段と、前記情報を前記スクランブル鍵によりスクランブルしたスクランブル情報を生成するスクランブル手段と、前記デスクランブル鍵と、前記スクランブル情報をデスクランブルするための所定の条件とを用いて、前記スクランブル情報をデスクランブルするための条件付き鍵を生成する条件付き鍵生成手段と、前記スクランブル情報と前記条件付き鍵とを出力する出力手段とを有し、前記情報デスクランブル装置は、前記スクランブル情報と、前記条件付き鍵とを入力する入力手段と、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成手段と、前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出手段と、前記デスクランブル鍵抽出手段により前記デスクランブル鍵が抽出されたか否かを判定する判定手段と、前記判定手段により前記デスクランブル鍵が抽出されたと判定された時に、抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記情報を抽出するデスクランブル手段と、デスクランブルされた前記情報を出力する出力手段とを有する。

【００２０】また、鍵管理システムは、前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、前記デスクランブル鍵抽出候補条件生成手段は、現在日時を前記デスクランブル鍵抽出候補条件として生成し、前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件生成手段で生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出する構成を成す。

【００２１】また、鍵管理システムは、前記情報スクランブル装置において、前記情報を複数の前記情報デスクランブル装置側に対して出力するにあたり、前記情報デスクランブル装置に対応して、前記デスクランブル鍵と、前記条件付き鍵とのいずれかを選択する鍵選択手段を有し、前記出力手段は、前記鍵選択手段で選択された前記デスクランブル鍵と前記条件付き鍵とのいずれかを出力し、前記情報デスクランブル装置はさらに、入力手段が前記デスクランブル鍵を入力した場合に前記デスクランブル鍵の前記デスクランブル手段への出力を行う切

り換え手段を有し、前記デスクランブル手段は、前記切り換え手段から入力した前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルする構成を成す。

【００２２】また、鍵管理システムは、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む第１の情報及び第２の情報を入力し、前記第１の情報をスクランブルしたスクランブル情報と、前記第２の情報とを出力する情報スクランブル装置と、前記スクランブル情報と前記第２の情報とを入力し、前記スクランブル情報をデスクランブルして出力する情報デスクランブル装置とからなる鍵管理システムであって、前記情報スクランブル装置は、前記第１の情報と、前記第２の情報と、前記第１の情報のスクランブルを行うスクランブル鍵と、スクランブルされた前記第１の情報のデスクランブルを行うデスクランブル鍵とを入力する入力手段と、前記第１の情報を前記スクランブル鍵によりスクランブルしたスクランブル情報を生成するスクランブル手段と、前記デスクランブル鍵と、前記スクランブル情報をデスクランブルするための所定の条件とを用いて、前記スクランブル情報をデスクランブルするための条件付き鍵を生成する条件付き鍵生成手段と、前記第２の情報への前記デスクランブル鍵の多重と、前記スクランブル情報への前記条件付き鍵の多重とをそれぞれ行う多重手段と、前記多重手段により多重された前記スクランブル情報と、前記多重手段により多重された前記第２の情報とを出力する出力手段とを有し、前記情報デスクランブル装置は、前記スクランブル情報または前記第２の情報を入力する入力手段と、前記入力手段に前記スクランブル情報が入力された場合に、前記スクランブル情報と前記スクランブル情報に多重された前記条件付き鍵との分離と、前記入力手段に前記第２の情報が入力された場合に、前記第２の情報と前記第２の情報に多重された前記デスクランブル鍵との分離とを行う分離手段と、前記入力手段に前記スクランブル情報が入力された場合に、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出候補条件を生成するデスクランブル鍵抽出候補条件生成手段と、前記デスクランブル鍵抽出候補条件が前記スクランブル情報をデスクランブルする所定の条件を満たす場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出するデスクランブル鍵抽出手段と、前記デスクランブル鍵抽出手段により前記デスクランブル鍵が抽出されたか否かを判定する判定手段と、前記判定手段により前記デスクランブル鍵が抽出されたと判定された時に、前記デスクランブル鍵抽出手段により抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記第１の情報の抽出と、前記分離手段により前記デスクランブル鍵が分離された場合には、前記入力手段に前記スクランブル情報が入力された時に、前記分離手段により前記第２の情報から分離された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルし前記第１の情報の抽出とをそれぞれ行うデスクランブル手段とを有する。

【００２３】また、鍵管理システムは、前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、前記デスクランブル鍵抽出候補条件生成手段は、現在日時を前記デスクランブル鍵抽出候補条件として生成し、前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件生成手段で生成された現在日時が前記スクランブル情報の公開許可日時を満足する場合にのみ、前記条件付き鍵から前記デスクランブル鍵を抽出し、前記デスクランブル手段は、前記入力手段に前記スクランブル情報が入力された時に、抽出された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルする構成を成す。

【００２４】また、鍵管理システムは、前記デスクランブル装置においてさらに、前記入力手段により入力した前記スクランブル情報及び前記第２の情報を記録する記録手段を有し、前記分離手段は、前記記録手段により記録された前記第２の情報を読み出し、前記第２の情報と前記第２の情報に多重された前記デスクランブル鍵を分離し、前記デスクランブル手段は、前記記録手段により記録された前記スクランブル情報を読み出し、前記分離手段により前記第２の情報から分離された前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルする構成を成す。

【００２５】また、鍵管理システムは、前記スクランブル情報をデスクランブルする所定の条件が前記スクランブル情報の公開許可日時であり、前記多重手段は、前記第２の情報に前記デスクランブル鍵の代わりに前記スクランブル情報の公開許可日時を表す情報を多重し、前記情報デスクランブル装置において、前記分離手段は、前記記録手段により記録された前記第２の情報を読み出し、前記第２の情報と、前記第２の情報に多重された前記公開許可日時を分離し、前記デスクランブル鍵抽出手段は、分離された前記公開許可日時を用いて、前記分離手段により分離した前記条件付き鍵から前記デスクランブル鍵を抽出し、前記デスクランブル手段は、前記記録手段により記録された前記スクランブル情報を読み出し、抽出された前記デスクランブル鍵を用いて、前記スクランブル情報をデスクランブルする構成を成す。

【００２６】また、鍵管理システムは、前記情報スクランブル装置においてさらに、前記第１の情報と前記第２の情報とを符号化する符号化手段と、符号化する前の前記第２の情報の一部をスクランブル鍵として生成するスクランブル鍵生成手段とを有し、前記スクランブル手段は、前記スクランブル鍵生成手段で生成されたスクランブル鍵により符号化された前記第１の情報をスクランブルし前記スクランブル情報を生成し、前記出力手段は、符号化した前記第２の情報と、前記スクランブル情報と

を出力し、前記情報デスクランブル装置はさらに、前記デスクランブル手段により抽出された前記第１の情報と、前記第２の情報とを復号化する復号化手段と、復号化された前記第２の情報の一部をデスクランブル鍵として分離するデスクランブル鍵分離手段とを有し、前記デスクランブル手段は、前記デスクランブル鍵分離手段により分離した前記デスクランブル鍵を用いて前記スクランブル情報をデスクランブルして前記第１の情報を抽出し、前記復号化手段は、抽出された前記第１の情報を復号化する構成を成す。

【００２７】また、鍵管理システムは、前記第１の情報は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせを含む番組であり、前記第２の情報は、画像と音声と前記画像及び前記音声以外のデータの単独又は組み合わせを含む広告である構成を成す。

【００２８】また、鍵管理システムは、前記条件付き鍵生成手段は、前記スクランブル情報をデスクランブルする所定の条件を鍵として、前記デスクランブル鍵をスクランブルし前記条件付き鍵を生成し、前記デスクランブル鍵抽出手段は、前記デスクランブル鍵抽出候補条件を鍵として、前記条件付き鍵をデスクランブルする構成を成す。

【００２９】また、鍵管理システムは、前記情報スクランブル装置は、前記スクランブル情報を複数の前記情報デスクランブル装置に対して出力するにあたり、前記条件付き鍵生成手段は、前記情報デスクランブル装置毎にそれぞれ異なる条件で前記スクランブル情報をデスクランブルするための前記条件付き鍵をそれぞれ生成する構成を成す。

【００３０】また、鍵管理システムは、前記条件付き鍵生成手段は、画像と音声と前記画像及び前記音声以外のデータとの単独又は組み合わせで構成される要素毎にそれぞれ異なる条件で前記スクランブル情報をデスクランブルするための前記条件付き鍵をそれぞれ生成する構成を成す。

【００３１】

【発明の実施の形態】以下、図面を使用して本発明の実施の形態を詳細に説明する。

【００３２】（実施の形態１）図１は、本発明の実施の形態１である鍵管理システムにおける情報スクランブル装置及び情報デスクランブル装置の構成図である。

【００３３】図中、１０１は情報をスクランブルして出力する情報スクランブル装置であり、１１１は情報スクランブル装置からの出力されたスクランブル化された情報をデスクランブルして出力する情報デスクランブル装置である。

【００３４】まず、情報スクランブル装置１０１の構成について以下に説明する。１０２は、画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報と、情報をスクランブルするスクランブル鍵と、

情報をスクランブルしたスクランブル情報をデスクランブルするデスクランブル鍵と、スクランブル情報をデスクランブル可能とする条件とを入力する入力部である。１０３は、入力部１０２で入力された情報を、スクランブル鍵によりスクランブルしスクランブル情報を生成するスクランブル部である。１０４は、入力部１０２で入力されたデスクランブル鍵を入力された条件においてのみスクランブル情報をデスクランブル可能とする鍵である条件付き鍵を生成する条件付き鍵生成部である。１０５は、条件付き鍵と、スクランブル情報とを出力する出力部である。

【００３５】次に、情報デスクランブル装置１１１の構成について以下に説明する。１１２は、スクランブル化されたスクランブル情報と、条件付き鍵とを入力する入力部である。１１３は、入力部１１２で入力された条件付き鍵からデスクランブル鍵を抽出するための候補条件を生成するデスクランブル鍵抽出候補条件生成部である。１１４は、抽出された候補条件により条件付き鍵からデスクランブル鍵を抽出するデスクランブル鍵抽出部である。１１５は、デスクランブル鍵抽出部１１４によりデスクランブル鍵が抽出されたかどうか判定する判定部である。１１６は、判定部１１５によりデスクランブル鍵が抽出されたと判定された時に、抽出されたデスクランブル鍵を用いて、入力部１１２で入力されたスクランブル情報をデスクランブルするデスクランブル部である。１１７は、デスクランブル部１１６でデスクランブルされた情報を出力する出力部である。

【００３６】次に、実施の形態１における鍵管理システムの具体的な動作について説明する。

【００３７】まず、情報スクランブル装置１０１の動作について図２を用いて説明する。

【００３８】入力部１０２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報を入力する（Ｓ２０１）。次に入力部１０２によりＳ２０１で入力した情報をデスクランブル可能とする条件を入力する（Ｓ２０２）。次に入力部１０２によりＳ２０１で入力した情報のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ２０３）。次にスクランブル部１０３によりＳ２０３で入力したスクランブル鍵を用いて入力した情報をスクランブルする（Ｓ２０４）。次に条件付き鍵生成部１０４によりＳ２０１で入力した条件においてのみデスクランブル鍵の抽出を可能とする条件付き鍵を生成する（Ｓ２０５）。次に出力部１０５によりＳ２０４でスクランブルされたスクランブル情報と、Ｓ２０５で生成された条件付き鍵を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ２０１へ戻る（Ｓ２０６）。

【００３９】次に、情報デスクランブル装置１１１の動作について図３を用いて説明する。

【００４０】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を入力する（Ｓ３０１）。次に入力部１１２により条件付き鍵を入力する（Ｓ３０２）。次にデスクランブル鍵抽出候補条件生成部１１３により条件付き鍵からのデスクランブル鍵の抽出を可能とする条件の候補を生成する（Ｓ３０３）。次にデスクランブル鍵抽出部１１４によりＳ３０３で生成した候補条件を用いて条件付き鍵からのデスクランブル鍵の抽出を行う（Ｓ３０４）。次に判定部１１５によりＳ３０４でデスクランブル鍵の抽出ができているかどうかの判定を行い、デスクランブル鍵の抽出ができていればＳ３０６の処理を行い、抽出ができていない場合はＳ３０３へ戻り、再度別の候補条件を生成する（Ｓ３０５）。次にデスクランブル部１１６によりＳ３０４で抽出されたデスクランブル鍵によりＳ３０１で入力した情報をデスクランブルする（Ｓ３０６）。次に出力部１１７によりＳ３０６でデスクランブルされた情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ３０１へ戻る（Ｓ３０７）。

【００４１】また、Ｓ３０１～Ｓ３０５の各ステップを実行するプログラムを記録媒体に記録し、情報デスクランブル装置が読み取り実行してもよい。

【００４２】以上説明した動作により、スクランブルした情報と条件付き鍵とを相手先に提供し、情相手先側で条件付き鍵からデスクランブル鍵が抽出できたときに情報をデスクランブルして使用することが出来る。従って、条件付き鍵の生成方法によって相手先に対して情報を公開する条件を情報の発信者側で制御することが出来る。

【００４３】なお、所定の条件においてのみスクランブル情報のデスクランブルを可能とする条件付き鍵の生成において、前述した説明においては条件が１種類であったが複数種類の条件を設けてもよい。その場合、条件として、情報スクランブル装置が出力するデータを入力する情報デスクランブル装置毎に異なる条件を用いてもよい。また、複数の要素で構成された情報をスクランブルして出力する際に、条件として複数の要素毎に異なる条件を用いてもよい。

【００４４】条件として情報の公開を許可する日時を用いる場合の情報スクランブル装置１０１の動作について図４を用いて説明する。

【００４５】入力部１０２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報を入力する（Ｓ４０１）。次に入力部１０２によりＳ４０１で入力した情報をデスクランブル可能とする条件として情報の公開許可日時を入力する（Ｓ４０２）。次に入力部１０２によりＳ４０１で入力した情報のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ４０３）。次にスクランブル部１０３によりＳ４０３で入力したスクランブル鍵を用いて入力した情報をスクランブルする（Ｓ４０４）。次に条件付き鍵生成部１０４によりＳ４０１で入力した公開許可日時においてのみデスクランブル鍵の抽出を可能とする条件付き鍵を生成する（Ｓ４０５）。次に出力部１０５によりＳ４０４でスクランブルされたスクランブル情報と、Ｓ４０５で生成された条件付き鍵を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ４０１へ戻る（Ｓ４０６）。

【００４６】条件として情報の公開を許可する日時を用いる場合の情報デスクランブル装置１１１の動作について図５を用いて説明する。

【００４７】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を入力する（Ｓ５０１）。次に入力部１１２により条件付き鍵を入力する（Ｓ５０２）。次にデスクランブル鍵抽出候補条件生成部１１３により条件付き鍵からのデスクランブル鍵の抽出を可能とする条件の候補として現在日時を生成する（Ｓ５０３）。次にデスクランブル鍵抽出部１１４によりＳ５０３で生成した現在日時が情報の公開許可日時を満たす場合にのみ条件付き鍵からのデスクランブル鍵の抽出を行う（Ｓ５０４）。次に判定部１１５によりＳ５０４でデスクランブル鍵の抽出ができているかどうかの判定を行い、デスクランブル鍵の抽出ができていればＳ５０６の処理を行い、抽出ができていない場合はＳ５０３へ戻り、再度別の候補条件を生成する（Ｓ５０５）。次にデスクランブル部１１６によりＳ５０４で抽出されたデスクランブル鍵によりＳ５０１で入力した情報をデスクランブルする（Ｓ５０６）。次に出力部１１７によりＳ５０６でデスクランブルされた情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ５０１へ戻る（Ｓ５０７）。

【００４８】また、Ｓ５０１～Ｓ５０５の各ステップを実行するプログラムを記録媒体に記録し、情報デスクランブル装置が読み取り実行してもよい。

【００４９】以上説明した動作により、情報を公開する日時を鍵としてデスクランブル鍵をスクランブルして条件付き鍵を生成する。相手先では現在日時が公開する日時になったときに条件付き鍵からデスクランブル鍵を再生し、情報をデスクランブルすることが出来る。公開する日時以前にスクランブルした情報を相手先に提供できるため、情報の発信者側で公開日時を管理する必要がない。また、公開日時に情報を提供した全ての相手先に同時に情報を公開することが出来る。相手先に提供する情報に公開日時情報を付与する必要がない。公開日時になった時点でネットワークや無線などの伝送媒体を用いて鍵情報を取得する必要がない。

【００５０】条件を鍵としてスクランブルし条件付き鍵

21

を生成する場合の情報スクランブル装置１０１の動作について図６を用いて説明する。

【００５１】入力部１０２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報を入力する（Ｓ６０１）。次に入力部１０２によりＳ６０１で入力した情報をデスクランブル可能とする条件を入力する（Ｓ６０２）。次に入力部１０２によりＳ６０１で入力した情報のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ６０３）。次にスクランブル部１０３によりＳ６０３で入力したスクランブル鍵を用いて入力した情報をスクランブルする（Ｓ６０４）。次に条件付き鍵生成部１０４によりＳ６０１で入力したデスクランブル鍵を条件を鍵としてスクランブルした条件付き鍵を生成する（Ｓ６０５）。次に出力部１０５によりＳ６０４でスクランブルされたスクランブル情報と、Ｓ６０５で生成された条件付き鍵を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ６０１へ戻る（Ｓ６０６）。

【００５２】条件を鍵としてスクランブルし生成された条件付き鍵を入力した場合の情報デスクランブル装置１１１の動作について図７を用いて説明する。

【００５３】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を入力する（Ｓ７０１）。次に入力部１１２により条件付き鍵を入力する（Ｓ７０２）。次にデスクランブル鍵抽出候補条件生成部１１３により条件付き鍵からのデスクランブル鍵の抽出を可能とする条件の候補を生成する（Ｓ７０３）。次にデスクランブル鍵抽出部１１４によりＳ７０３で生成した候補条件を鍵としてスクランブル情報のデスクランブルを行うことによりデスクランブル鍵の抽出を行う（Ｓ７０４）。次に判定部１１５によりＳ７０４でデスクランブル鍵の抽出ができているかどうかの判定を行い、デスクランブル鍵の抽出ができていればＳ７０６の処理を行い、抽出ができていない場合はＳ７０３へ戻り、再度別の候補条件を生成する（Ｓ７０５）。次にデスクランブル部１１６によりＳ７０４で抽出されたデスクランブル鍵によりＳ７０１で入力した情報をデスクランブルする（Ｓ７０６）。次に出力部１１７によりＳ７０６でデスクランブルされた情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ７０１へ戻る（Ｓ７０７）。

【００５４】また、Ｓ７０１～Ｓ７０５の各ステップを実行するプログラムを記録媒体に記録し、情報デスクランブル装置が読み取り実行してもよい。

【００５５】なお、スクランブル情報をデスクランブル可能とする条件を鍵としてスクランブルし条件付き鍵を生成する場合に、条件を情報の公開許可日時としてもよい。この場合の情報スクランブル装置の動作としては、

22

Ｓ６０２において情報の公開許可日時を入力し、Ｓ６０５において公開許可日時を鍵としてデスクランブル鍵をデスクランブルし条件付き鍵を生成する。また、情報デスクランブル装置の動作としては、Ｓ７０３において現在日時を候補条件として生成し、Ｓ７０４において現在日時を鍵として条件付き鍵をデスクランブルすることでデスクランブル鍵を抽出する。

【００５６】また、前述した説明においては条件が１種類であったが複数種類の条件を鍵として条件付き鍵を生成してもよい。その場合、条件として、情報スクランブル装置が出力するデータを入力する情報デスクランブル装置毎に異なる条件を鍵としてデスクランブル鍵をスクランブルし条件付き鍵を生成してもよい。これにより、情報を提供する相手先によって異なる条件付き鍵を提供することが出来る。従って、米国のように国内で時差があるような国において全国に情報を配信し、それを同時に公開することが出来る。ある場所を基準として公開日時を決め、配信先と基準となる場所との時差から実際に公開する日時を決定し、その値でデスクランブル鍵をスクランブルする。これにより、配信先に時差がある場合でも情報の同時公開を保証することが出来る。

【００５７】また、複数の要素で構成された情報をスクランブルして出力する際に、条件として複数の要素毎に異なる条件を用いてもよい。これにより、情報を構成する要素毎に公開する日時の異なる条件付き鍵を相手先に提供することが出来る。例えば通信販売の商品リストにおいて、毎週変わる特売商品のデータに対してはその日だけ有効な条件付き鍵を提供する。これにより、提供する情報の要素毎に公開日時を変更することが出来る。

【００５８】（実施の形態２）図８は、本発明の実施の形態２である鍵管理システムにおける情報スクランブル装置及び情報デスクランブル装置の構成図である。

【００５９】図中、実施の形態１と同じ構成要素については同一番号を付与しているので説明は省略する。以下、実施の形態２で新たな構成について説明する。情報スクランブル装置１０１内の、８０１は、入力部１０２で入力したデスクランブル鍵かあるいは条件付き鍵生成部で生成した条件付き鍵かのいずれか一方を選択し、出力部１０５へ出力する鍵選択部である。

【００６０】また、情報デスクランブル装置内の、８１１は入力された鍵がデスクランブル鍵の場合は、１１６のデスクランブル部においてスクランブル情報を入力されたデスクランブル鍵を用いてスクランブル情報をデスクランブルし、入力された鍵が条件付き鍵なら実施の形態１と同様にデスクランブル鍵抽出候補条件生成部１１３で候補条件を生成し、デスクランブル鍵抽出部１１４において生成された候補条件によりデスクランブル鍵を抽出するように入力された鍵に応じて処理の切り換えを切り換え部である。

【００６１】次に、実施の形態２における鍵管理システ

ムの具体的な動作について説明する。

【００６２】まず、情報スクランブル装置１０１の動作について図９を用いて説明する。

【００６３】入力部１０２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報を入力する（Ｓ９０１）。次に入力部１０２によりＳ９０１で入力した情報をデスクランブル可能とする条件を入力する（Ｓ９０２）。次に入力部１０２によりＳ９０１で入力した情報のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ９０３）。次にスクランブル部１０３によりＳ９０３で入力したスクランブル鍵を用いて入力した情報をスクランブルする（Ｓ９０４）。次に条件付き鍵生成部１０４によりＳ９０１で入力した条件においてのみデスクランブル鍵の抽出を可能とする条件付き鍵を生成する（Ｓ９０５）。次に鍵選択部８０１によりＳ９０３により入力されたデスクランブル鍵と、Ｓ９０５により生成された条件付き鍵のうちいずれか一方を選択する（Ｓ９０６）。次に出力部１０５によりＳ９０４でスクランブルされたスクランブル情報と、Ｓ９０６で選択されたデスクランブル鍵かあるいは条件付き鍵を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ９０１へ戻る（Ｓ９０７）。

【００６４】次に、情報デスクランブル装置１１１の動作について図１０を用いて説明する。

【００６５】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む情報をスクランブルしたスクランブル情報を入力する（Ｓ１００１）。次に入力部１１２によりデスクランブル鍵あるいは条件付き鍵を入力する（Ｓ１００２）。次に切り換え部８１１によりＳ１００２で入力された鍵がデスクランブル鍵の場合は、Ｓ１００７の処理を行い、Ｓ１００２で入力された鍵が条件付き鍵の場合は、Ｓ１００４の処理を行う（Ｓ１００３）。デスクランブル鍵抽出候補条件生成部１１３により条件付き鍵からのデスクランブル鍵の抽出を可能とする条件の候補を生成する（Ｓ１００４）。次にデスクランブル鍵抽出部１１４によりＳ１００４で生成した候補条件を用いて条件付き鍵からのデスクランブル鍵の抽出を行う（Ｓ１００５）。次に判定部１１５によりＳ１００５でデスクランブル鍵の抽出ができているかどうかの判定を行い、デスクランブル鍵の抽出ができていればＳ１００７の処理を行い、抽出ができていない場合はＳ１００４へ戻り、再度別の候補条件を生成する（Ｓ１００６）。次にデスクランブル部１１６によりデスクランブル鍵を用いてＳ１００１で入力した情報をデスクランブルする（Ｓ１００７）。次に出力部１１７によりＳ１００７でデスクランブルされた情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１００１へ戻る（Ｓ１００８）。

【００６６】また、Ｓ１００１～Ｓ１００６の各ステップを実行するプログラムを記録媒体に記録し、情報デスクランブル装置が読み取り実行してもよい。

【００６７】なお、スクランブル情報をデスクランブル可能とする条件を鍵としてスクランブルし条件付き鍵を生成する場合に、条件を情報の公開許可日時としてもよい。具体的な動作は実施の形態１と同様の動作となる。

【００６８】また、所定の条件においてのみスクランブル情報のデスクランブルを可能とする条件付き鍵の生成において、前述した説明においては条件が１種類であったが複数種類の条件を設けてもよい。その場合、条件として、情報スクランブル装置が出力するデータを入力する情報デスクランブル装置毎に異なる条件を用いてもよい。また、複数の要素で構成された情報をスクランブルして出力する際に、条件として複数の要素毎に異なる条件を用いてもよい。

【００６９】以上説明した動作により、情報を提供する相手先によってデスクランブル鍵を提供するか、条件付き鍵を提供するかを選択することが出来る。従って、例えば電子音楽配信サービスなどにおいてまだ楽曲を購入していないリスナーに対して１回だけ聴くことができる楽曲を配信することにより、楽曲を聴く機会を与え、結果として楽曲の宣伝効果及び販売促進に貢献することが出来る。

【００７０】（実施の形態３）図１１は、本発明の実施の形態３である鍵管理システムにおける情報スクランブル装置及び情報デスクランブル装置の構成図である。

【００７１】図中、実施の形態１または２と同じ構成要素については同一番号を付与している。

【００７２】まず、情報スクランブル装置１０１の構成について以下に説明する。入力部１０２は、画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第１の情報及び第２の情報と、第１の情報のスクランブルとを行うスクランブル鍵と、スクランブルされた第１の情報のデスクランブルを行うデスクランブル鍵とを入力する。スクランブル部１０３は、第１の情報をスクランブル鍵によりスクランブルしスクランブル情報を生成する。条件付き鍵生成部１０４は、入力部１０２で入力されたデスクランブル鍵を入力された条件においてのみスクランブル情報をデスクランブル可能とする鍵である条件付き鍵を生成する。１１０１は、実施の形態３で新たに加わった構成要素であり、第２の情報へのデスクランブル鍵の多重と、スクランブル情報への条件付き鍵の多重とを行う多重部である。出力部１０５は、１１０１で多重されたスクランブル情報と、第２の情報とを出力する。

【００７３】次に、情報デスクランブル装置１１１の構成について以下に説明する。入力部１１２は、スクランブル化されたスクランブル情報または、第２の情報を入力する。１１１１は、実施の形態３で新たに加わった構

成要素であり、入力部１１２でスクランブル情報が入力された場合にはスクランブル情報と多重されている条件付き鍵との分離を行い、第２の情報が入力された場合には第２の情報と多重されているデスクランブル鍵との分離を行う分離部である。分離部１１１１においてスクランブル情報から条件付き鍵の分離が行われた場合には、分離された情報付き鍵を用いて、実施の形態１と同様にデスクランブル鍵抽出候補条件生成部１１３、デスクランブル鍵抽出部１１４、判定部１１５、デスクランブル部１１６によりデスクランブルされた情報を抽出する。分離部１１１１において第２の情報からのデスクランブル鍵の分離が行われた場合には、分離されたデスクランブル鍵を用いてデスクランブル部１１６によりデスクランブルされた情報を抽出する。

【００７４】次に、実施の形態３における鍵管理システムの具体的な動作について説明する。

【００７５】まず、情報スクランブル装置１０１の動作について図１２を用いて説明する。入力部１０２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第１の情報及び第２の情報を入力する（Ｓ１２０１）。次に入力部１０２によりＳ１２０１で入力した第１の情報をデスクランブル可能とする条件を入力する（Ｓ１２０２）。次に入力部１０２によりＳ１２０１で入力した第１の情報のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ１２０３）。次にスクランブル部１０３によりＳ１２０３で入力したスクランブル鍵を用いて入力した第１の情報をスクランブルする（Ｓ１２０４）。次に条件付き鍵生成部１０４によりＳ１２０１で入力した条件においてのみデスクランブル鍵の抽出を可能とする条件付き鍵を生成する（Ｓ１２０５）。次に多重部１１０１によりＳ１２０４でスクランブルされたスクランブル情報に、Ｓ１２０５により生成された条件付き鍵を多重する（Ｓ１２０６）。また多重部１１０１では第２の情報に、デスクランブル鍵を多重する（Ｓ１２０７）。次に出力部１０５によりＳ１２０６で多重されたスクランブル情報と、Ｓ１２０７で多重された第２の情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１２０１へ戻る（Ｓ１２０８）。

【００７６】次に、情報デスクランブル装置１１１の動作について図１３を用いて説明する。

【００７７】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第１の情報をスクランブルしたスクランブル情報または第２の情報を入力し、入力がスクランブル情報であればＳ１３０２へ処理を移し、入力が第２の情報であればＳ１３０４へ処理を移す（Ｓ１３０１）。分離部１１１１により、入力が第２の情報の場合、第２の情報から多重されているデスクランブル鍵を分離しＳ１３０１へ処理を移す（Ｓ１３０４）。入力がスクランブル情報の場合、デスクランブル鍵が抽出されたかを判定し、Ｓ１３０４により第２の情報からデスクランブル鍵が既に抽出済みの場合にはＳ１３０８へ処理を移し、まだ抽出されていない場合には、Ｓ１３０３へ処理を移す（Ｓ１３０２）。分離部１１１１により、スクランブル情報が入力された場合に、スクランブル情報から条件付き鍵を分離する（Ｓ１３０３）。次にデスクランブル鍵抽出候補条件生成部１１３により分離された条件付き鍵からのデスクランブル鍵の抽出を可能とする条件の候補を生成する（Ｓ１３０５）。次にデスクランブル鍵抽出部１１４によりＳ１３０５で生成した候補条件を用いて条件付き鍵からのデスクランブル鍵の抽出を行う（Ｓ１３０６）。次に判定部１１５によりＳ１３０６でデスクランブル鍵の抽出ができているかどうかの判定を行い、デスクランブル鍵の抽出ができていればＳ１３０８の処理を行い、抽出ができていない場合はＳ１３０５へ戻り、再度別の候補条件を生成する（Ｓ１３０７）。次にデスクランブル部１１６によりデスクランブル鍵を用いてＳ１３０１で入力したスクランブル情報をデスクランブルする（Ｓ１３０８）。次に出力部１１７によりＳ１３０８でデスクランブルされた第１の情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１３０１へ戻る（Ｓ１３０９）。

【００７８】なお、スクランブル情報をデスクランブル可能とする条件を鍵としてスクランブルし条件付き鍵を生成する場合に、条件を第１の情報の公開許可日時としてもよい。具体的な動作は実施の形態１と同様の動作となる。

【００７９】また、条件を鍵としてデスクランブル鍵をスクランブルして条件付き鍵を生成し、デスクランブル鍵の抽出時においても候補条件を鍵としてデスクランブルすることによりデスクランブル鍵を抽出してもよい。具体的な動作は実施の形態１と同様の動作となる。

【００８０】また、所定の条件においてのみスクランブル情報のデスクランブルを可能とする条件付き鍵の生成において、前述した説明においては条件が１種類であったが複数種類の条件を設けてもよい。その場合、条件として、情報スクランブル装置が出力するデータを入力する情報デスクランブル装置毎に異なる条件を用いてもよい。また、複数の要素で構成された情報をスクランブルして出力する際に、条件として複数の要素毎に異なる条件を用いてもよい。

【００８１】次に実施の形態３において第１の情報が番組であり、第２の情報がＣＭである場合について具体的な動作を説明する。

【００８２】まず、情報スクランブル装置１０１の具体的な動作を図１４と図１６を用いて説明する。

【００８３】入力部１０２により番組及びＣＭを入力する（Ｓ１４０１）。次に入力部１０２によりＳ１４０１

で入力した番組をデスクランブル可能とする条件を入力する（Ｓ１４０２）。次に入力部１０２によりＳ１４０１で入力した番組のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ１４０３）。次にスクランブル部１０３によりＳ１４０３で入力したスクランブル鍵を用いて入力した番組をスクランブルする（Ｓ１４０４）。次に条件付き鍵生成部１０４によりＳ１４０１で入力した条件においてのみデスクランブル鍵の抽出を可能とする条件付き鍵を生成する（Ｓ１４０５）。次に多重部１１０１によりＳ１４０４でスクランブルされたスクランブル情報に、Ｓ１４０５により生成された条件付き鍵を多重する（Ｓ１４０６）。また多重部１１０１ではＣＭに、デスクランブル鍵を多重する（Ｓ１４０７）。次に出力部１０５によりＳ１４０６で多重されたスクランブル情報と、Ｓ１４０７で多重されたＣＭを出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１４０１へ戻る（Ｓ１４０８）。多重部１１１１から出力される情報は、図１６に示したようになる。スクランブル化された番組１６０２をデスクランブルするためのデスクランブル鍵１６０３をＣＭ１６０１へ多重し、番組１６０２に番組１６０２をデスクランブルするデスクランブル鍵を抽出可能な条件付き鍵１６０４が多重されている。

【００８４】次に、情報デスクランブル装置１１１の動作について図１５を用いて説明する。

【００８５】入力部１１２により番組をスクランブルしたスクランブル情報またはＣＭを入力し、入力がスクランブル情報であればＳ１５０２へ処理を移し、入力がＣＭであればＳ１５０４へ処理を移す（Ｓ１５０１）。分離部１１１１により、入力がＣＭの場合、ＣＭから多重されているデスクランブル鍵を分離しＳ１５０１へ処理を移す（Ｓ１５０４）。入力が番組である場合、デスクランブル鍵が抽出されたかを判定し、Ｓ１５０４によりＣＭからデスクランブル鍵が既に抽出済みの場合にはＳ１５０８へ処理を移し、まだ抽出されていない場合には、Ｓ１５０３へ処理を移す（Ｓ１５０２）。分離部１１１１により、番組のスクランブル情報が入力された場合に、スクランブル情報から条件付き鍵を分離する（Ｓ１５０３）。次にデスクランブル鍵抽出候補条件生成部１１３により分離された条件付き鍵からのデスクランブル鍵の抽出を可能とする条件の候補を生成する（Ｓ１５０５）。次にデスクランブル鍵抽出部１１４によりＳ１５０５で生成した候補条件を用いて条件付き鍵からのデスクランブル鍵の抽出を行う（Ｓ１５０６）。次に判定部１１５によりＳ１５０６でデスクランブル鍵の抽出ができているかどうかの判定を行い、デスクランブル鍵の抽出ができていればＳ１５０８の処理を行い、抽出ができていない場合はＳ１５０５へ戻り、再度別の候補条件を生成する（Ｓ１５０７）。次にデスクランブル部１１６によりデスクランブル鍵を用いてＳ１５０１で入力した番組のスクランブル情報をデスクランブルし番組を抽出する（Ｓ１５０８）。次に出力部１１７によりＳ１５０８でデスクランブルされた番組を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１５０１へ戻る（Ｓ１５０９）。

【００８６】なお、番組をデスクランブル可能とする条件を鍵としてスクランブルし条件付き鍵を生成する場合に、条件を番組の公開許可日時としてもよい。具体的な動作は実施の形態１と同様の動作となる。

【００８７】また、条件を鍵としてデスクランブル鍵をスクランブルして条件付き鍵を生成し、デスクランブル鍵の抽出時においても候補条件を鍵としてデスクランブルすることによりデスクランブル鍵を抽出してもよい。具体的な動作は実施の形態１と同様の動作となる。

【００８８】また、所定の条件においてのみ番組のデスクランブルを可能とする条件付き鍵の生成において、前述した説明においては条件が１種類であったが複数種類の条件を設けてもよい。その場合、条件として、情報スクランブル装置が出力するデータを入力する情報デスクランブル装置毎に異なる条件を用いてもよい。また、複数の要素で構成された番組をスクランブルして出力する際に、条件として番組の複数の要素毎に異なる条件を用いてもよい。

【００８９】以上説明したように実施の形態３によると、情報デスクランブル装置側では番組に多重された条件付き鍵からデスクランブル鍵を抽出し、番組をデスクランブルして出力することが出来る。この時、ＣＭに多重されたデスクランブル鍵を必要とせず、番組を視聴することができる。このため、番組の途中から視聴を開始した場合でも直ちに番組を視聴することが出来る。

【００９０】（実施の形態４）図１７は、本発明の実施の形態４である鍵管理システムにおける情報スクランブル装置及び情報デスクランブル装置の構成図である。

【００９１】図中、実施の形態３と同じ構成要素については同一番号を付与している。実施の形態３と異なるのは、情報デスクランブル装置において、第１の情報及び第２の情報を記憶する記憶部１７０１が加わっていることである。これにより、分離部１１１１は、記録部１７０１に記録された第２の情報を読み出し、第２の情報と多重されたデスクランブル鍵を分離する。また、デスクランブル部１１６は、記録部に記録されたスクランブル情報を読み出し、分離部１１１１で分離されたデスクランブル鍵を用いてスクランブル情報をデスクランブルし第１の情報を抽出する。

【００９２】次に、実施の形態４における鍵管理システムの具体的な動作について説明する。情報スクランブル装置１０１の動作は、実施の形態３と同じであるため説明を省略する。情報デスクランブル装置１１１の動作について図１８を用いて説明する。

【００９３】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第１の情報をスクランブルしたスクランブル情報または第２の情報を入力し、スクランブル情報及び第２の情報を記録部１７０１へ記録する（Ｓ１８０１）。次に分離部１１１１により、記録部１７０１で記録されている第２の情報を読み出し、第２の情報から多重されているデスクランブル鍵を分離する（Ｓ１８０２）。次に分離部１１１１により、記録部１７０１で記録されている第１の情報をスクランブルしたスクランブル情報を読み出し、スクランブル情報と多重されている条件付き鍵を分離する（Ｓ１８０３）。デスクランブル部１１６は、分離部１１１１で分離されたデスクランブル鍵を用いて分離されたスクランブル情報をデスクランブルする（Ｓ１８０４）。次に出力部１１７によりＳ１８０４でデスクランブルされた第１の情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１８０１へ戻る（Ｓ１８０５）。以上説明したように、情報を一旦記録して処理する場合には、記録部１７０１に記録された第１の情報をスクランブルしたスクランブル情報に多重された条件付き鍵は使用しないこととなる。

【００９４】次に実施の形態４において、第１の情報が番組であり、第２の情報がＣＭである場合の動作について説明する。

【００９５】情報スクランブル装置１０１の動作は、実施の形態３で説明した動作と同じである。

【００９６】情報デスクランブル装置１１１の動作は、上記説明において第１の情報を番組として第２の情報をＣＭと置き換えたものとなり、記録部１７０１で記録されたＣＭを読み出し、ＣＭに多重されているデスクランブル鍵を分離部１１１１により分離し、分離したデスクランブル鍵を用いて記録部１７０１で記録された番組をデスクランブルして出力することとなる。

【００９７】次に実施の形態４において、条件が第１の情報の公開許可日時であり、第２の情報のデスクランブル鍵の代わりに第１の情報の公開許可日時を多重した場合について具体的な動作を説明する。

【００９８】まず、情報スクランブル装置１０１の具体的な動作を図１９を用いて説明する。

【００９９】入力部１０２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第１の情報及び第２の情報を入力する（Ｓ１９０１）。次に入力部１０２によりＳ１９０１で入力した第１の情報の公開許可日時を入力する（Ｓ１９０２）。次に入力部１０２によりＳ１９０１で入力した第１の情報のスクランブルを行うスクランブル鍵と、スクランブル化されたスクランブル情報のデスクランブルを行うデスクランブル鍵とを入力する（Ｓ１９０３）。次にスクランブル部１０３によりＳ１９０３で入力したスクランブル鍵を用いて入力した第１の情報をスクランブルする（Ｓ１９０４）。次に条件付き鍵生成部１０４によりＳ１９０１で入力した第１の情報の公開許可日時を満たす場合においてのみデスクランブル鍵の抽出を可能とする条件付き鍵を生成する（Ｓ１９０５）。次に多重部１１０１によりＳ１２０４でスクランブルされたスクランブル情報に、Ｓ１９０５により生成された条件付き鍵を多重する（Ｓ１９０６）。また多重部１１０１では第２の情報に、公開許可日時を多重する（Ｓ１９０７）。次に出力部１０５によりＳ１９０６で多重されたスクランブル情報と、Ｓ１９０７で多重された第２の情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ１９０１へ戻る（Ｓ１９０８）。

【０１００】次に、情報デスクランブル装置１１１の具体的な動作を図２０を用いて説明する。

【０１０１】入力部１１２により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第１の情報をスクランブルしたスクランブル情報または第２の情報を入力し、記録部１７０１へ記録する（Ｓ２００１）。分離部１１１１により、記録部１７０１に記録されている第２の情報を読み出し、第２の情報から多重されている公開許可日時を分離する（Ｓ２００２）。分離部１１１１により、記録部１７０１に記録されているスクランブル情報を読み出し、スクランブル情報から条件付き鍵を分離する（Ｓ２００３）。次にデスクランブル鍵抽出部１１４によりＳ２００２で分離された公開許可日時を用いて条件付き鍵からのデスクランブル鍵の抽出を行う（Ｓ２００４）。次にデスクランブル部１１６によりデスクランブル鍵を用いてスクランブル情報をデスクランブルし第１の情報を抽出する（Ｓ２００５）。次に出力部１１７によりＳ２００５でデスクランブルされた第１の情報を出力し、出力が終了したら終了し、出力が終了していなければ、Ｓ２００１へ戻る（Ｓ２００６）。

【０１０２】また、実施の形態４において、第１の情報が番組であり、第２の情報がＣＭであり、条件が第１の情報の公開許可日時であり、第２の情報のデスクランブル鍵の代わりに第１の情報の公開許可日時を多重した場合について具体的な動作は、図１９及び図２０を用いて説明した動作において、第１の情報を番組、第２の情報をＣＭと置き換えた場合の動作となる。

【０１０３】なお、実施の形態４において、条件を鍵としてデスクランブル鍵をスクランブルし条件付き鍵を生成し、条件つき鍵からのデスクランブル鍵の抽出は、条件を鍵として条件付き鍵をデスクランブルしてデスクランブル鍵を抽出してもよい。またこの時の条件として公開許可日時を用いてもよい。

【０１０４】また、条件が１種類であったが複数種類の条件を鍵として条件付き鍵を生成してもよい。その場合、条件として、情報スクランブル装置が出力するデータを入力する情報デスクランブル装置毎に異なる条件を

鍵としてデスクランブル鍵をスクランブルし条件付き鍵を生成してもよい。また、複数の要素で構成された情報をスクランブルして出力する際に、条件として複数の要素毎に異なる条件を用いてもよい。

【0105】以上のように実施の形態4によると、情報デスクランブル装置側では、蓄積された番組を視聴する（タイムシフト視聴）場合は、まずCMを視聴してデスクランブル鍵を取得しないと番組をデスクランブルすることが出来ない。従って、タイムシフト視聴時でも視聴者がCMを視聴することが保証できる。

【0106】（実施の形態5）図21は、本発明の実施の形態5である鍵管理システムにおける情報スクランブル装置及び情報デスクランブル装置の構成図である。

【0107】図21に実施の形態5の鍵管理システムの構成は、実施の形態4の構成に対して、情報スクランブル装置において、第1の情報及び第2の情報を符号化する符号化部2101と、第2の情報の一部を第1の情報のスクランブル鍵とするスクランブル鍵生成部2102とが加わり、また、情報デスクランブル装置において、符号化された第1の情報及び第2の情報を復号化する復号化部2111と、第2の情報の一部をデスクランブル鍵として分離するデスクランブル鍵分離部2112とが加わっている。

【0108】ここでいう符号化とは、例えば、MPEG（Moving Picture Experts Group）などのような圧縮符号化技術を用いることができる。

【0109】次に、実施の形態5の鍵管理システムにおいて情報を一旦蓄積し出力する場合の、具体的な動作について説明する。

【0110】まず、情報スクランブル装置101の動作について図22及び図24を用いて説明する。

【0111】入力部102により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第1の情報及び第2の情報を入力する（S2201）。次にスクランブル鍵生成部2102により第2の情報の一部を取り出し、第1の情報をスクランブルするスクランブル鍵として生成する（S2202）。デスクランブル鍵を生成する方法として、図24で示すように、第2の情報の最終部分のデータのビット列を使用してもよい。次に符号化部2101により、第1の情報及び第2の情報を符号化する（S2203）。第2の情報を符号化する際に、図24に示すように、IGOP（Group Of Picture）で圧縮符号化してもよい。次にスクランブル部103により符号化された第1の情報をスクランブル鍵生成部2102で生成されたスクランブル鍵を用いてスクランブルする（S2204）。次に出力部105によりスクランブル部103で第1の情報をスクランブルしたスクランブル情報と、符号化部2101で符号化された第2の情報とを出力し、出力が終了したら終了し、出力が終了していなければ、S1201へ戻る（S2205）。

【0112】次に、情報デスクランブル装置111の動作について図23を用いて説明する。

【0113】入力部112により画像と、音声と、画像及び音声以外のデータとの単独又は組み合わせを含む第1の情報をスクランブルしたスクランブル情報と第2の情報とを入力し、記録部1701へ記録する（S2301）。次にデスクランブル鍵分離部2112により、記録部1701に記録されている第2の情報を読み出し、復号化部2111へ第2の情報を出力し復号化された第2の情報を再入力し、第2の情報の一部を抜き出してデスクランブル鍵として生成する（S2302）。次にデスクランブル部116は、記録部1701からスクランブル情報を読み出し、デスクランブル鍵分離手段で生成されたデスクランブル鍵を用いてスクランブル情報をデスクランブルし第1の情報を抽出する（S2303）。次に復号化部2111によりデスクランブル部116で抽出された第1の情報を復号化する（S2304）。次に出力部117によりS2304で復号化された第1の情報を出力し、出力が終了したら終了し、出力が終了していなければ、S2301へ戻る（S2305）。

【0114】次に実施の形態5において、情報デスクランブル装置が第1の情報を蓄積せずに出力する場合の具体的動作は、情報スクランブル装置は、スクランブル鍵生成部2102で生成されたスクランブル鍵を元に、入力部102で入力された条件に対して条件付き鍵生成部104で条件付き鍵を生成し、符号化されさらにスクランブル化された第1の情報に対して多重部101において条件付き鍵を多重し出力することとなる。また、情報デスクランブル装置においては、実施の形態3で説明した動作と同様に第1の情報をデスクランブルし、その後デスクランブルされた第1の情報を復号化部2111で復号し出力することとなる。

【0115】次に実施の形態5において、第1の情報が番組であり、第2の情報がCMである場合の具体的な動作は、図22及び図23で説明した動作において、第1の情報を番組、第2の情報をCMとして置き換えた動作となる。

【0116】以上のように実施の形態5によると、番組をスクランブルする際のスクランブル鍵としてCMの一部のデータを使用し、そのCMを圧縮符号化してから出力する。情報デスクランブル装置側でタイムシフト視聴を行う際には、番組を視聴する前にまずCMを読み出し、圧縮符号化されたCMを伸長して圧縮符号化する前のデータの一部からデスクランブル鍵を取得しなければ番組をデスクランブルして視聴することが出来ない。また、CMのデータの最後のデータのビット列を使用しデスクランブル鍵を生成し、CMを1GOPで圧縮符号化した場合には、番組を視聴する前にCMを先頭から最後

まで視聴してからでないと番組を視聴することが出来ない。これにより、蓄積されたデータからデスクランブル鍵だけを抽出してＣＭを飛ばして視聴することを防ぐことが出来る。

【０１１７】（実施の形態６）図２７は、本発明の実施の形態６である鍵管理システムにおける情報スクランブル装置及び情報デスクランブル装置の構成図である。

【０１１８】図中、実施の形態１～５と同じ構成要素については同一番号を付与している。

【０１１９】図中、スクランブル部１０３は入力された番組の情報をスクランブル鍵によってスクランブルする。

【０１２０】条件付き鍵生成部１０４は有料番組を放送する日時を鍵としてデスクランブル鍵を更にスクランブルする。

【０１２１】ＳＷ２７０２はデスクランブル鍵と条件付き鍵の何れかを選択し、出力する。

【０１２２】２７０３の鍵スクランブル部２はデスクランブル鍵をスクランブル化するワーク鍵Ｋｗと受信契約者との契約情報とをマスタ鍵Ｋｍを鍵として暗号化する。Ｋｍは受信契約者毎に固有の鍵情報である。

【０１２３】２７０４の鍵スクランブル部２はＳＷ２７０２が出力するデスクランブル鍵又は条件付き鍵をＫｗを鍵としてスクランブルする。

【０１２４】多重部１１０１はＣＭと、スクランブル部１０３でスクランブルされた番組と、２７０４の鍵スクランブル部２が出力した情報と、２７０３の鍵スクランブル部１が出力した情報とを多重する。

【０１２５】出力制御部２７０１はＳＷ２７０２及び多重部１１０１の動作を制御する。

【０１２６】記録部１７０１は、放送された番組及びＣＭを一時記録する。

【０１２７】入力部１１２は放送された番組及びＣＭと、記録部１７０１に記録された番組及びＣＭの何れかを選択し、分離部１１１１に出力する。

【０１２８】分離部１１１１は、放送された情報から番組とＣＭとスクランブルされた鍵情報とに分離する。

【０１２９】２７１１の鍵デスクランブル部１はスクランブルされた鍵情報をマスタ鍵Ｋｍを鍵として復号化する。

【０１３０】２７１２の鍵デスクランブル部２はスクランブルされた鍵情報を２７１２の鍵デスクランブル部１でデスクランブルしたワーク鍵Ｋｗを鍵としてデスクランブルする。

【０１３１】デスクランブル鍵抽出候補条件生成部１１３は現在の日時をデスクランブル鍵の抽出条件として生成する。

【０１３２】デスクランブル抽出部１１４はデスクランブル鍵抽出候補条件生成部１１３で生成された現在の日時を鍵として条件付き鍵をデスクランブルする。

【０１３３】判定部１１５はデスクランブル鍵抽出部１１４でデスクランブル鍵が抽出されたかを判定し、抽出できていればデスクランブル鍵を出力し、抽出できていなければ再度デスクランブル鍵抽出候補条件生成部１１３において別の条件である現在日時を生成させる。

【０１３４】ＳＷ２７１４は２７１２の鍵デスクランブル部１の出力とデスクランブル鍵抽出部１１４の出力の何れかを選択し、デスクランブル鍵を出力する。

【０１３５】視聴判定部２７１５はデスクランブル鍵及び契約情報から、視聴者が正式に受信契約をしているかどうかを判定する。

【０１３６】デスクランブル部１１６は暗号化された番組をデスクランブル鍵を鍵としてデスクランブルする。

【０１３７】出力部１１７はデスクランブルされた番組とＣＭとを多重し、出力する。

【０１３８】端末制御部２７１３は入力部１１２と分離部１１１１と出力部１１７の動作を制御する。

【０１３９】図２７の情報デスクランブル装置１１１において、点線で示した部分２７１６は通常ＩＣカード等の記録媒体の形態で実現される。視聴者は受信契約を行った際に放送事業者からＩＣカード２７１６を受け取り、情報デスクランブル装置１１１に挿入することによって有料番組を視聴することが出来る。

【０１４０】次に、実施の形態６における鍵管理システムの動作について説明する。まず、情報スクランブル装置１０１の動作について図２８を用いて説明する。

【０１４１】放送する番組及びＣＭは、通常ＭＰＥＧ（Ｍｏｖｉｎｇ Ｐｉｃｔｕｒｅ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）などのような圧縮符号化技術を用いて符号化されている。放送する番組を選択し（ステップＳ２８０１）、それがＣＭ付き有料番組である場合（ステップＳ２８０２、２８０３）、放送する番組をスクランブル部１０３に入力し、スクランブルする（ステップＳ２８０７）。このとき、スクランブル鍵を用いる。また、スクランブル化された番組をデスクランブルするデスクランブル鍵は条件付き鍵生成部１０４に入力される。条件付き鍵生成部１０４はデスクランブル鍵をスクランブルして条件付き鍵を生成する（ステップＳ２８０８）。また、放送する有料番組の放送日時をデスクランブル鍵スクランブルするときの鍵とする。

【０１４２】ＳＷ２７０２で選択されたデスクランブル鍵或いは条件付き鍵は、２７０４の鍵スクランブル部２でスクランブルされる（ステップＳ２８０５、２８０９）。このとき、ワーク鍵Ｋｗを鍵として用いる。

【０１４３】Ｋｗは受信契約者との契約情報と共に２７０３の鍵スクランブル部１でスクランブルされる（ステップＳ２８１６）。このとき、マスタ鍵Ｋｍを用いてスクランブルする。Ｋｍは受信者毎に固有の鍵情報である。

【０１４４】ＣＭと、スクランブル部１０３でスクランブルされた番組と、スクランブルされた条件付き鍵及びデスクランブル鍵と、スクランブルされたＫｗ及び契約情報とは多重部１１０１で多重される。入力がＣＭであるか、番組であるかを判定し（ステップＳ２８０４）、ＣＭを出力するときは、出力制御部２７０１はデスクランブル鍵を出力するようＳＷ２７０２に指示し、多重部１１０１にはＣＭとデスクランブル鍵とを多重して出力するよう指示する。これにより、ＣＭとデスクランブル鍵とが多重される（ステップＳ２８０６）。一方、番組を出力するときは出力制御部２７０１は条件付き鍵を出力するようＳＷ２７０２に指示し、多重部１１０１には番組と条件付き鍵とを多重して出力するよう指示する。これにより、番組と条件付き鍵とが多重される（ステップＳ２８１０）。多重部１１０１はさらに上記番組とＣＭと暗号化されたＫｗ及び契約情報とを多重する（ステップＳ２８１７）。

【０１４５】鍵に関する情報は例えばＭＰＥＧ－ＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）のＣＡ（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ）セクションにマッピングされ、ＴＳパケットを構成する。このパケットは、番組及びＣＭの映像及び音声のＴＳパケットと多重され、トランスポートストリームが生成される。

【０１４６】多重部１１０１から出力される情報は図１６に示したようになる。番組１６０２のスクランブルを解除する鍵のうち、デスクランブル鍵１６０３はＣＭ１６０１に多重される。一方、条件付き鍵１６０４は番組１６０２に多重される。

【０１４７】選択した番組がＣＭなしの有料番組である場合は、スクランブル部１０３で番組をスクランブルする（ステップＳ２８１１）。出力制御部２７０１はデスクランブル鍵を出力するようＳＷ２７０２に指示し、多重部１１０１には番組とスクランブル鍵を多重するよう指示する。その結果、デスクランブル鍵が２７０４の鍵スクランブル部２に入力される。２７０４の鍵スクランブル部２はデスクランブル鍵をワーク鍵Ｋｗで暗号化する（ステップＳ２８１２）。多重部１１０１はスクランブルされた番組とデスクランブル鍵とを多重する（ステップＳ２８１３）。ワーク鍵Ｋｗは契約情報と共に２７０３の鍵スクランブル部１においてマスタ鍵Ｋｍで暗号化され（ステップＳ２８１８）、多重部１１０１で番組及びデスクランブル鍵と共に多重される（ステップＳ２８１９）。

【０１４８】選択した番組が無料番組である場合は、出力制御部２７０１の指示により、スクランブル部１０３は機能を停止し（ステップＳ２８１４）、入力された番組をそのまま出力する（ステップＳ２８１５）。

【０１４９】次に、情報デスクランブル装置１１１の動作について説明する。まず、オンエアされた番組及びＣＭを直ちに視聴する場合の動作について図２９を用いて説明する。

【０１５０】視聴者は視聴するチャネルを選択し（ステップＳ２９０１）、選択したチャネルで放送されている番組がＣＭ付きの有料番組である場合（ステップＳ２９０２、２９０３）、入力部１１２は端末制御部２７１３からの指示により、入力された（オンエアされた）番組及びＣＭを選択し、分離部１１１１に出力する。分離部１１１１は、入力された情報をＣＭと、スクランブルされた番組と、スクランブル化された鍵情報とに分離し、出力する。分離部１１１１は入力が番組である場合（ステップＳ２９０４）、番組に多重されたスクランブルされた条件付き鍵を分離して（ステップＳ２９０５）２７１２の鍵デスクランブル部２に出力する。

【０１５１】ＣＭとスクランブルされた番組との区別は、例えばＭＰＥＧ－ＴＳで符号化した場合、ＴＳパケットヘッダのｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌフィールドを参照し、スクランブルされているか、そうでないかを判定することによって区別することが出来る。

【０１５２】２７１１の鍵デスクランブル部１は分離部１１１１が出力するスクランブルされた鍵情報をデスクランブルし、ワーク鍵Ｋｗと契約情報とを出力する（ステップＳ２９０６）。２７１１の鍵デスクランブル部１はＩＣカード２７１６で管理されるマスタ鍵Ｋｍを用いて復号を行う。

【０１５３】また、２７１２の鍵デスクランブル部２は分離部１１１１が出力するスクランブルされた条件付き鍵をデスクランブルし、条件付き鍵を抽出する（ステップＳ２９０７）。２７１２の鍵デスクランブル部２は２７１１の鍵デスクランブル部１が出力するＫｗを用いてデスクランブルを行う。

【０１５４】復号された条件付き鍵はデスクランブル鍵抽出部１１４に入力される。デスクランブル鍵抽出部１１４は、デスクランブル鍵抽出候補条件生成部１１３が出力する現在の日時を鍵としたデスクランブラで構成される。

【０１５５】放送をオンエア時に直ちに視聴するときは、条件付き鍵がデスクランブラに入力されたときの日時と、条件付き鍵生成部１０４で条件付き鍵を生成したときの鍵（放送日時）とが等しい。従って、条件付き鍵をデスクランブル鍵抽出部１１４に入力すると、出力として条件付き鍵をスクランブルする前の情報、即ち番組をデスクランブルするために用いるデスクランブル鍵が出力される（ステップＳ２９０８）。ＳＷ２７１４は、デスクランブル鍵抽出部１１４でデスクランブル鍵の抽出ができたか否かを判定する判定部１１５により抽出ができたと判定された場合に、抽出されたデスクランブル鍵を選択し、視聴判定部２７１５に出力する。

【０１５６】視聴判定部２７１５では２７１１の鍵デスクランブル部１からの契約情報とＳＷ２７１４からのデ

スクランブル鍵とから正規の受信契約をした視聴者であるかどうかを判定し（ステップＳ２９０９）、正規の視聴者であると判定した場合にデスクランブル鍵をデスクランブル部１１６に出力する。デスクランブル部１１６は、視聴判定部２７１５が出力したデスクランブル鍵を用いて番組をデスクランブルする（ステップＳ２９１０）。出力部１１７はＣＭとデスクランブルされた番組とを切り替え、出力する（ステップＳ２９１１、２９１２）。

【０１５７】ＣＭなしの有料番組を視聴するとき、分離部１１１１は端末制御部２７１３からの指示により、放送された番組から鍵情報を分離する（ステップＳ２９１３）。スクランブルされたワーク鍵Ｋｗ及び契約情報は２７１１の鍵デスクランブル部１でマスタ鍵Ｋｍによってデスクランブルされる（ステップＳ２９１４）。２７１２の鍵デスクランブル部２はこのＫｗを用いてスクランブルされたデスクランブル鍵をデスクランブルし、デスクランブル鍵を再生する（ステップＳ２９１５）。ＳＷ２７１４は２７１２の鍵デスクランブル部２からの入力を選択し、デスクランブル鍵が視聴判定部２７１５に入力される。視聴判定部２７１５は２７１１の鍵デスクランブル部１からの契約情報とＳＷ２７１４からのデスクランブル鍵とから正規の受信契約をした視聴者であるかどうかを判定し（ステップＳ２９１６）、正規の視聴者であると判定した場合にＳＷ２７１４から入力されたデスクランブル鍵をデスクランブル部１１６に出力する。デスクランブル部１１６は、視聴判定部２７１５が出力したデスクランブルを用いて番組をデスクランブルする（ステップＳ２９１７）。出力部１１７はデスクランブルされた番組を出力する（ステップＳ２９１８）。

【０１５８】無料番組を視聴するとき、端末制御部２７１３は、デスクランブル部１１６の機能を停止するよう指示する（ステップＳ２９１９）。番組はそのまま出力部１１７を通って出力される（ステップＳ２９２０）。

【０１５９】以上の動作により、受信契約を行った視聴者は放送された番組に多重された条件付き鍵から万能鍵を再生し、番組をデスクランブルして視聴することが出来る。ＣＭに多重された万能鍵は必要ない。このため、番組の途中から視聴を開始した場合でも直ちに番組を視聴することが出来る。

【０１６０】次に、放送された番組を一旦蓄積し、任意の時間が経過した後に蓄積した番組を視聴する（タイムシフト視聴）場合の動作について図３０を用いて説明する。

【０１６１】入力部１１２は端末制御部２７１３からの指示により、入力された番組及びＣＭを記録部１７０１に記録する。記録部１７０１にはＣＭとスクランブルされた状態の番組と、スクランブルされた鍵情報とが記録される。記録部１７０１に記録された番組を再生するとき、入力部１１２は端末制御部２７１３の指示により、

記録部１７０１から必要な情報を読み出し（ステップＳ３００１）、分離部１１１１に出力する。端末制御部２７１３からの指示によって読み出した番組がＣＭ付き有料番組であると判定したとき（ステップＳ３００２、３００３）、分離部１１１１は入力された情報をＣＭと、スクランブルされた番組と、スクランブルされた鍵情報とに分離し、出力する。このとき、分離部１１１１はＣＭに多重されたデスクランブル鍵を２７１２の鍵デスクランブル部２に出力する。

【０１６２】記録部１７０１に記録された条件付き鍵は、記録部１７０１に記録された時点で無効データになる。なぜならば、条件付き鍵からデスクランブル鍵を再生するためにはデスクランブル鍵抽出部１１４にその番組が放送された日時が鍵として入力されなければならないからである。記録部１７０１に記録され、現在日時が放送日時と等しくなくなった時点で条件付き鍵からデスクランブル鍵を再生することが出来なくなる。従って、記録部１７０１に記録された番組を読み出して視聴するときは、ＣＭに多重されたデスクランブル鍵を２７１２の鍵デスクランブル復号部２に出力する。

【０１６３】入力部１１２は番組を視聴するに先立って、記録部１７０１からＣＭと、ＣＭに多重されたスクランブルされた鍵情報を読み出し、分離部１１１１に出力する。分離部１１１１はＣＭを検出し（ステップＳ３００４）、ＣＭとスクランブルされた鍵情報とを分離する（ステップＳ３００５）。分離されたＣＭは出力部１１７を経由して出力される（ステップＳ３０１２）。

【０１６４】２７１１の鍵デスクランブル部１は分離部１１１１が出力するスクランブルされた鍵情報をデスクランブルし、ワーク鍵Ｋｗと契約情報とを出力する（ステップＳ３００６）。２７１１の鍵デスクランブル部１はＩＣカード２７１６で管理されるマスタ鍵Ｋｍを用いて復号を行う。

【０１６５】また、２７１２の鍵デスクランブル部２は分離部１１１１が出力するスクランブルされたデスクランブル鍵をデスクランブルし、デスクランブル鍵を抽出する（ステップＳ３００８）。２７１２の鍵デスクランブル部２は２７１１の鍵デスクランブル部１が出力するＫｗを用いてデスクランブルを行う。

【０１６６】２７１２の鍵デスクランブル部２によって抽出されたデスクランブル鍵は、ＳＷ２７１４を通して視聴判定部２７１５に入力される。視聴判定部２７１５では２７１１の鍵デスクランブル部１からの契約情報とＳＷ２７１４からのデスクランブル鍵とから正規の受信契約をした視聴者であるかどうかを判定し、正規の受信契約者であると判定した場合にデスクランブル鍵をデスクランブル部１１６に出力する（ステップＳ３００８、３００９）。

【０１６７】ＣＭの読み出しが完了すると、入力部１１２は視聴判定部２７１５が出力するデスクランブル鍵に

対応する番組を記録部１７０１から読み出す。読み出された番組は分離部１１１１を通してデスクランブル部１１６に入力される。デスクランブル部１１６は、視聴判定部２７１５が出力したデスクランブル鍵を用いて番組をデスクランブルし（ステップＳ３０１０）、出力部１１７を通って出力する（ステップＳ３０１１）。

【０１６８】有料番組及び無料番組視聴時において、再生する番組を読み出した後の動作はオンエア視聴時の動作と同様である。

【０１６９】本実施例によれば、蓄積された番組を視聴する（タイムシフト視聴）場合は、まずＣＭを視聴して万能鍵を取得しないと番組をデスクランブルすることが出来ない。従って、タイムシフト視聴時でも視聴者がＣＭを視聴することが保証できる。

【０１７０】

【発明の効果】以上説明したように、本発明によれば以下のような効果が得られる。

【０１７１】スクランブルした情報と条件付き鍵とを相手先に提供し、相手先で条件付き鍵からデスクランブル鍵が再生できたときに情報をデスクランブルして使用することが出来る。従って、条件付き鍵の生成方法によって相手先に対して情報を公開する条件を情報の発信者側で制御することが出来る。

【０１７２】また、情報の公開を許可する日時を鍵としてデスクランブル鍵をスクランブルして条件付き鍵を生成する。相手先では現在日時が公開許可日時になったときに条件付き鍵からデスクランブル鍵を再生し、情報をデスクランブルすることが出来る。公開許可日時以前にスクランブルした情報を相手先に提供できるため、情報の発信者側で公開許可日時を管理する必要がない。また、公開許可日時に情報を提供した全ての相手先に同時に情報を公開することが出来る。相手先に提供する情報に公開許可日時情報を付与する必要がない。公開許可日時になった時点でネットワークや無線などの伝送媒体を用いて鍵情報を取得する必要がない。

【０１７３】また、情報を提供する相手先によって異なる条件付き鍵を提供することが出来る。従って、米国のように国内で時差があるような国において全国に情報を配信し、それを同時に公開することが出来る。ある場所を基準として公開日時を決め、配信先と基準となる場所との時差から実際に公開する日時を決定し、その値で万能鍵をスクランブルする。これにより、配信先に時差がある場合でも情報の同時公開を保証することが出来る。

【０１７４】また、情報を構成する要素毎に公開する日時の異なる条件付き鍵を相手先に提供することが出来る。例えば通信販売の商品リストにおいて、毎週変わる特売商品のデータに対してはその日だけ有効な条件付き鍵を提供する。これにより、提供する情報の要素毎に公開日時を変更することが出来る。

【０１７５】また、情報を提供する相手先によってデスクランブル鍵を提供するか、条件付き鍵を提供するかを選択することが出来る。従って、例えば電子音楽配信サービスなどにおいてまだ楽曲を購入していないリスナーに対して１日だけ聴くことができる楽曲を配信することにより、楽曲を聴く機会を与え、結果として楽曲の宣伝効果及び販売促進に貢献することが出来る。

【０１７６】また、ＣＭ付きの有料番組において、番組をスクランブルし、ＣＭに番組をデスクランブルするためのデスクランブル鍵を多重し、番組には放送日時を鍵としてデスクランブル鍵をスクランブルした条件付き鍵を多重して放送する。オンエア時に直ちに放送された番組を視聴する場合は番組に多重された条件付き鍵を現在日時を鍵としてデスクランブルし、デスクランブル鍵を抽出して番組をデスクランブルし、番組を視聴することが出来る。一方、番組を一旦記録して任意の時間経過後に記録された番組を視聴する（タイムシフト視聴）時には、番組に多重された条件付き鍵は無効となり、ＣＭを視聴してデスクランブル鍵を取得しないと番組をデスクランブルすることが出来ない。このため、タイムシフト視聴時にも視聴者がＣＭを見ることを保証でき、スポンサーの参入を促進して低料金で番組を提供することが出来る。また、オンエア時には番組の途中から視聴を開始した場合でも直ちに番組を視聴することが出来る。

【０１７７】また、ＣＭ及び番組を圧縮符号化して放送するにあたり、ＣＭを圧縮符号化する前のデータの一部を番組をスクランブルするデスクランブル鍵として使用する。番組にはデスクランブル鍵を放送日時でスクランブルした条件付き鍵を多重して放送する。従って、一旦蓄積した番組を読み出して視聴する場合はＣＭを伸長して視聴し、圧縮前のデータからデスクランブル鍵を取得しなければ番組をデスクランブルすることが出来ない。記録されたＣＭデータからある位置のビット列を抜き出すだけでは万能鍵を取得することが出来ないため、タイムシフト視聴時に視聴者がＣＭを見ることがより確実に保証できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における鍵管理システムの構成図

【図２】本発明の第１の実施の形態における情報スクランブル装置の具体的動作を説明する処理フロー図

【図３】本発明の第１の実施の形態における情報デスクランブル装置の具体的動作を説明する処理フロー図

【図４】本発明の第１の実施の形態において条件が公開許可日時である場合の情報スクランブル装置の具体的動作を説明する処理フロー図

【図５】本発明の第１の実施の形態において条件が公開許可日時である場合の情報デスクランブル装置の具体的動作を説明する処理フロー図

【図６】本発明の第１の実施の形態において条件を鍵として条件付き鍵を生成する場合の情報スクランブル装置

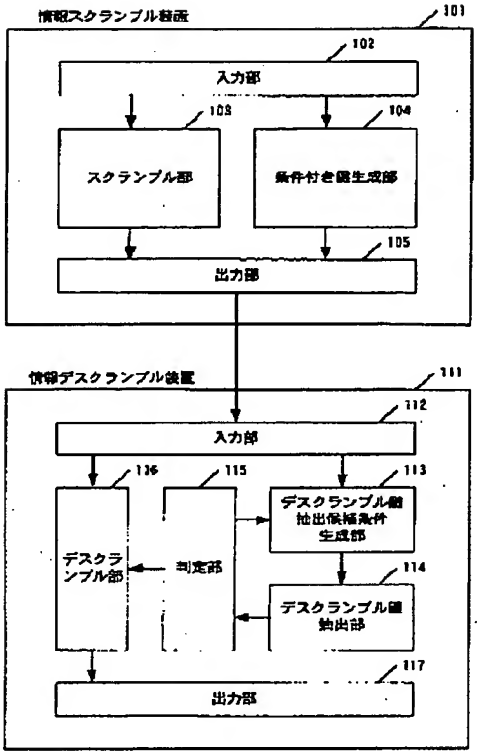
41

の具体的動作を説明する処理フロー図
【図７】本発明の第１の実施の形態において条件を鍵として生成した条件付き鍵を使用する場合の情報デスクランブル装置の具体的動作を説明する処理フロー図
【図８】本発明の第２の実施の形態における鍵管理システムの構成図
【図９】本発明の第２の実施の形態における情報スクランブル装置の具体的動作を説明する処理フロー図
【図１０】本発明の第２の実施の形態における情報デスクランブル装置の具体的動作を説明する処理フロー図
【図１１】本発明の第３の実施の形態における鍵管理システムの構成図
【図１２】本発明の第３の実施の形態における情報スクランブル装置の具体的動作を説明する処理フロー図
【図１３】本発明の第３の実施の形態における情報デスクランブル装置の具体的動作を説明する処理フロー図
【図１４】本発明の第３の実施の形態において番組とＣＭを出力する場合の情報スクランブル装置の具体的動作を説明する処理フロー図
【図１５】本発明の第３の実施の形態において番組とＣＭを入力する場合の情報デスクランブル装置の具体的動作を説明する処理フロー図
【図１６】本発明の第３の実施の形態におけるＣＭ及び番組に多重された鍵を説明する図
【図１７】本発明の第４の実施の形態における鍵管理システムの構成図
【図１８】本発明の第４の実施の形態における情報スクランブル装置の具体的動作を説明する処理フロー図
【図１９】本発明の第４の実施の形態において公開許可日時を多重する場合の情報スクランブル装置の具体的動作を説明する処理フロー図
【図２０】本発明の第４の実施の形態において公開許可日時を多重する場合の情報デスクランブル装置の具体的動作を説明する処理フロー図
【図２１】本発明の第５の実施の形態における鍵管理システムの構成図
【図２２】本発明の第５の実施の形態における情報スクランブル装置の具体的動作を説明する処理フロー図
【図２３】本発明の第５の実施の形態における情報デスクランブル装置の具体的動作を説明する処理フロー図
【図２４】本発明の第５の実施の形態における第２の情報とスクランブル鍵との関係とを説明する処理フロー図
【図２５】従来技術の構成図
【図２６】従来技術の具体的動作を説明するための図
【図２７】本発明の第６の実施の形態における鍵管理システムの構成図
【図２８】本発明の第５の実施の形態における情報スクランブル装置の具体的動作を説明する処理フロー図
【図２９】本発明の第５の実施の形態における情報デスクランブル装置の具体的動作を説明する処理フロー図
【図３０】本発明の第５の実施の形態においてタイムシフト視聴する場合の情報デスクランブル装置の具体的動作を説明する処理フロー図

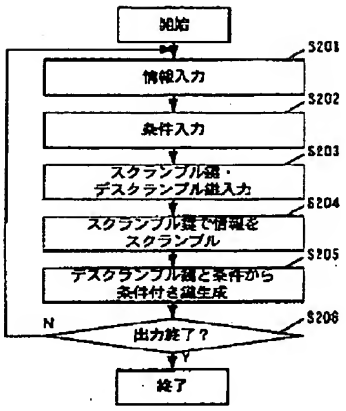
42

【符号の説明】
１０１，２５０１　情報スクランブル装置
１０２　入力部
１０３　スクランブル部
１０４　条件付き鍵生成部
１０５　出力部
１１１，２５２０　情報デスクランブル装置
１１２　入力部
１１３　デスクランブル鍵抽出候補条件生成部
１１４　デスクランブル鍵抽出部
１１５　判定部
１１６　デスクランブル部
１１７　出力部
８０１　鍵選択部
８１１　切り換え部
１１０１　多重部
１１１１　分離部
１７０１　記録部
２１０１　符号化部
２１０２　スクランブル鍵生成部
２１１１　復号化部
２１１２　デスクランブル鍵分離部
２５００　鍵管理装置
２５０１　スクランブル鍵，デスクランブル鍵管理テーブル
２５３０　ネットワーク
１６０１，２６０１，２６０２，２６０３　ＣＭ
１６０２，２６０７，２６０８，２６０９　番組
１６０３，２６０４，２６０５，２６０６　デスクランブル鍵
１６０４　条件付き鍵
２７０１　出力制御部
２７０２　ＳＷ
２７０３　鍵スクランブル部１
２７０４　鍵スクランブル部２
２７１１　鍵デスクランブル部１
２７１２　鍵デスクランブル部２
２７１３　端末制御部
２７１４　ＳＷ
２７１５　視聴判定部
２７１６　ＩＣカード

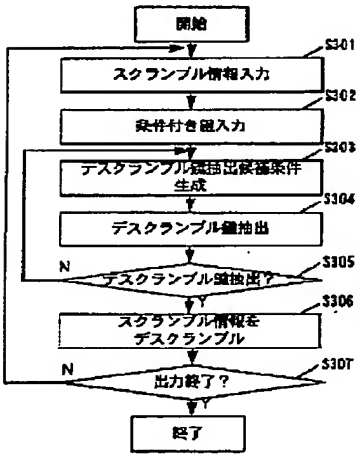
【図１】



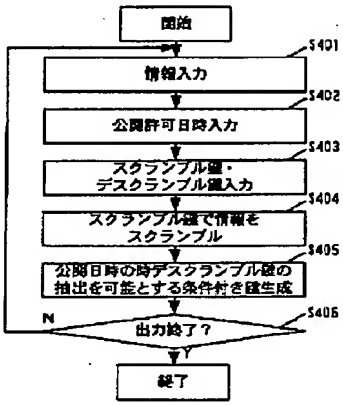
【図２】



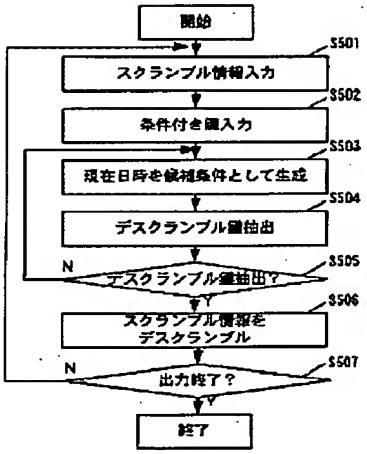
【図３】



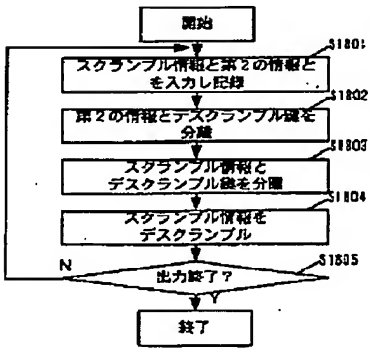
【図４】



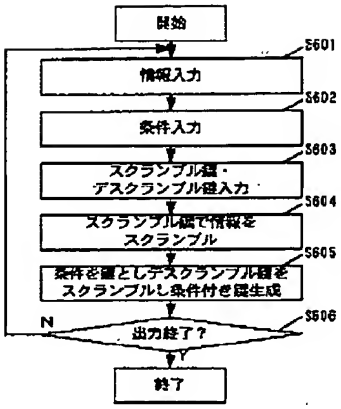
【図５】



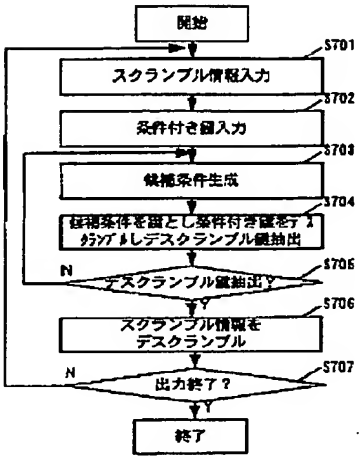
【図１８】



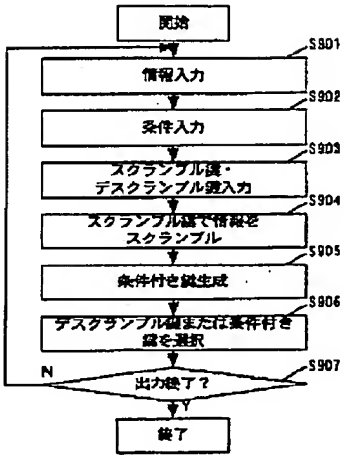
【図６】



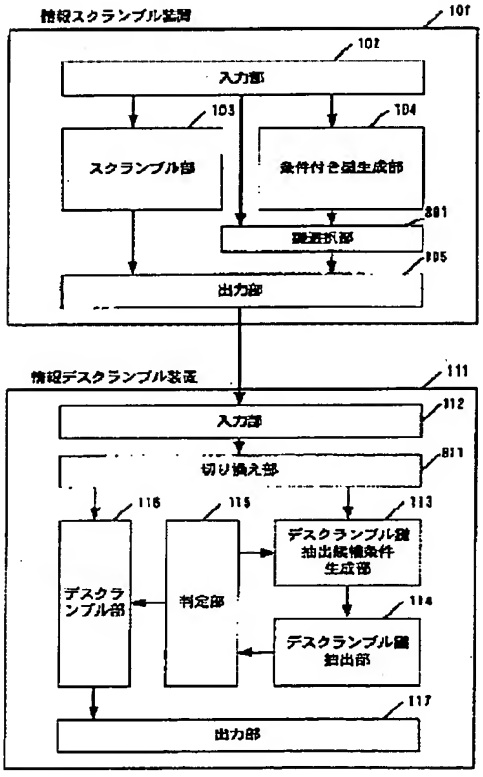
【図７】



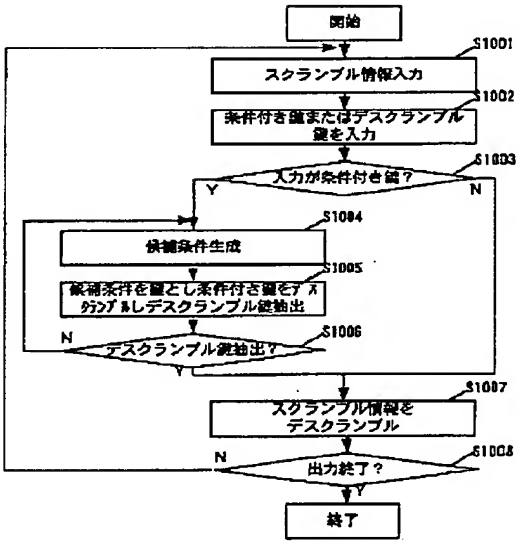
【図９】



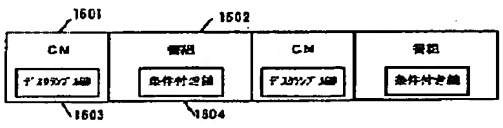
【図８】



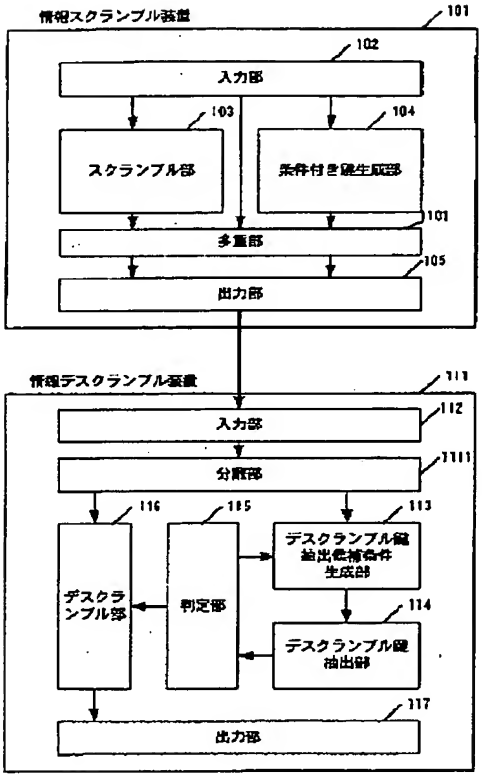
【図１０】



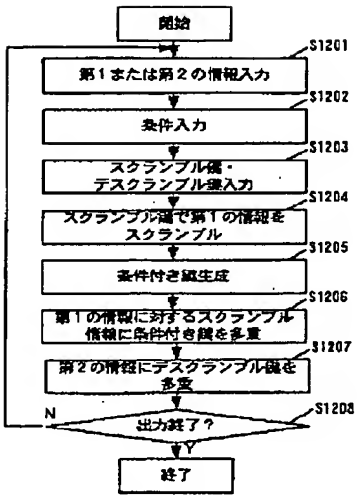
【図１６】



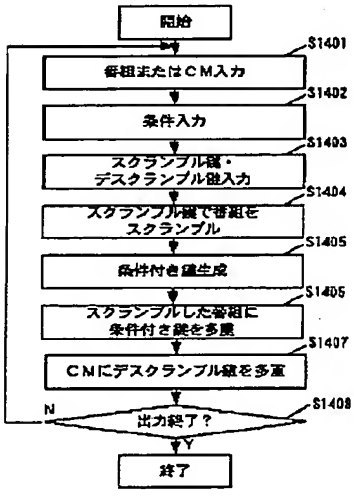
【図１１】



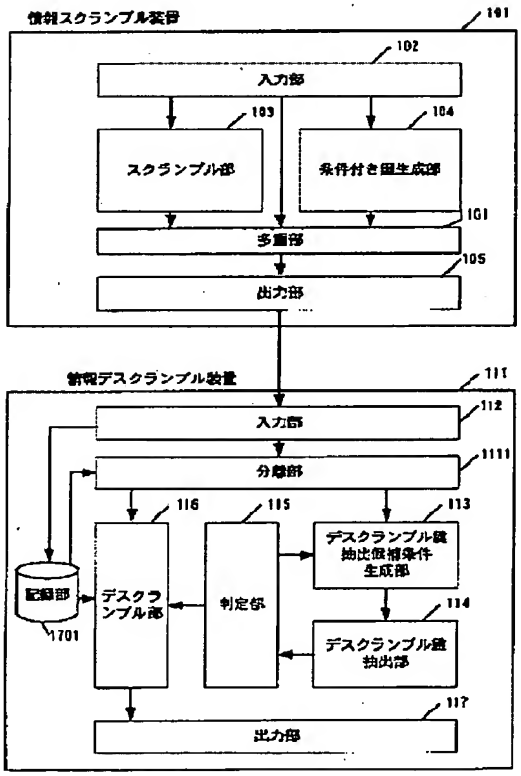
【図１２】



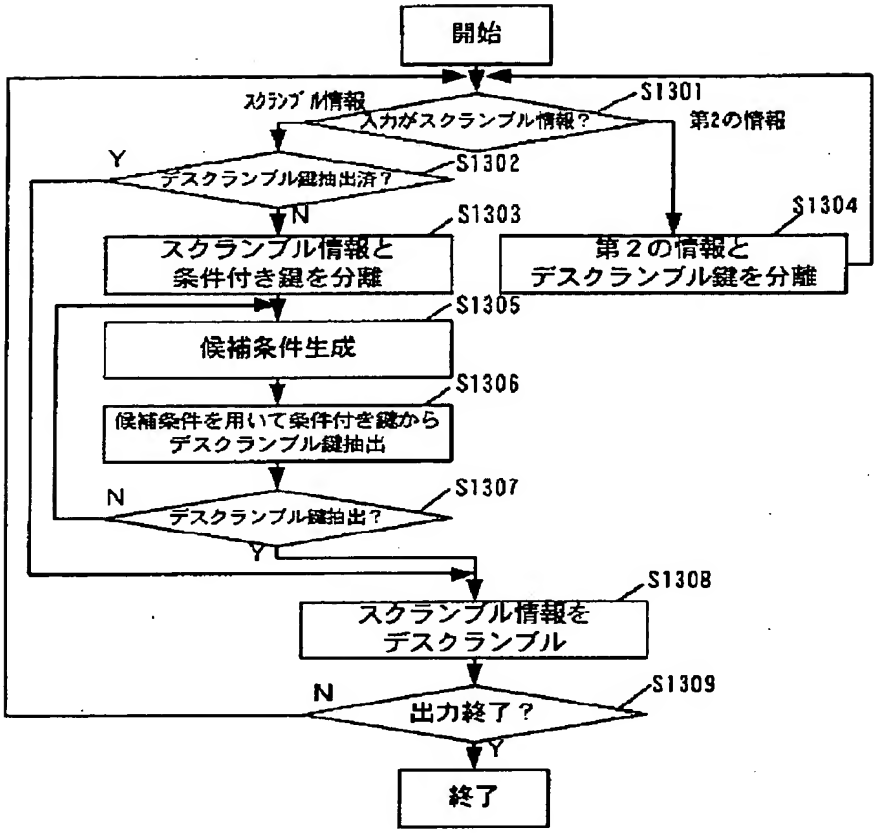
【図１４】



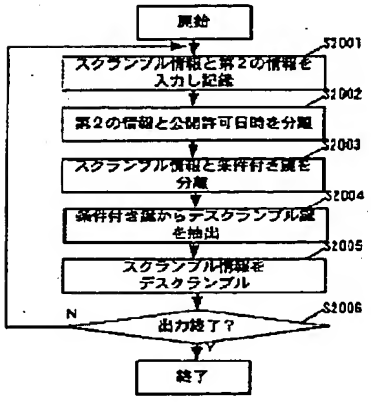
【図１７】



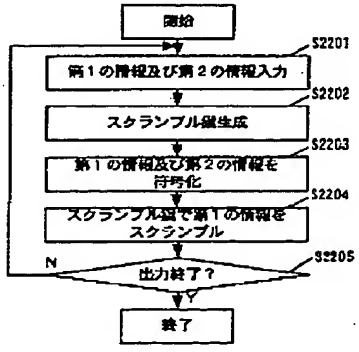
【図１３】



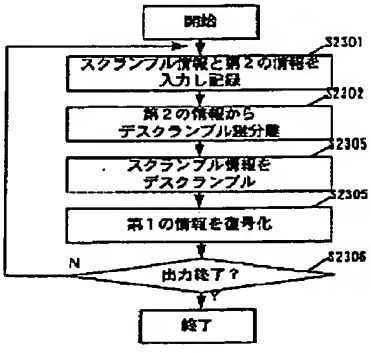
【図２０】



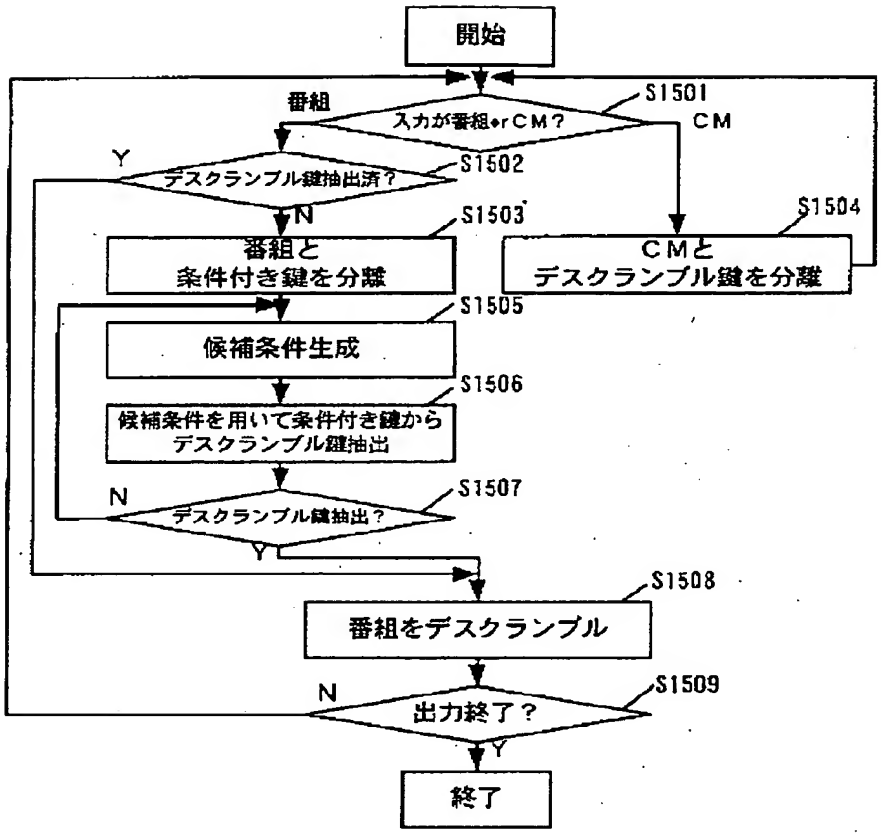
【図２２】



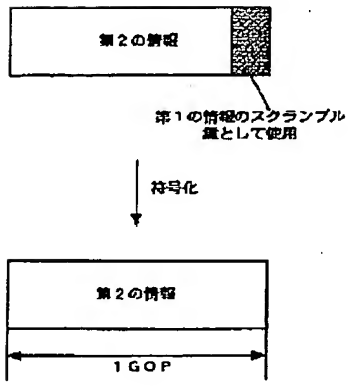
【図２３】



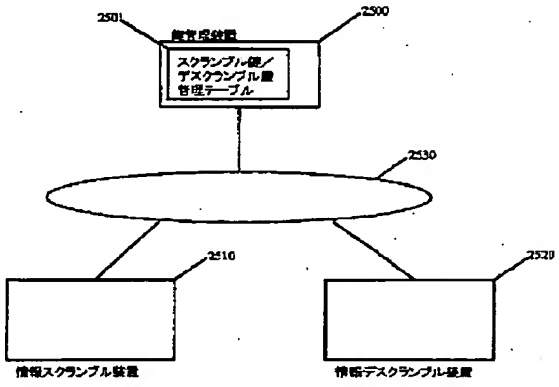
【図１５】



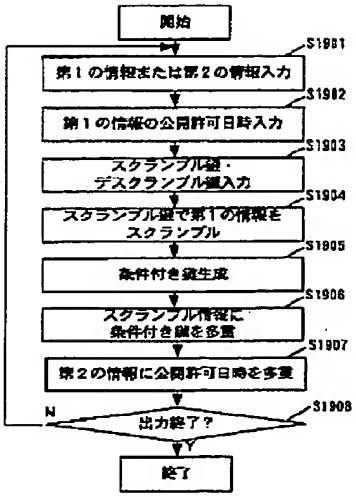
【図２４】



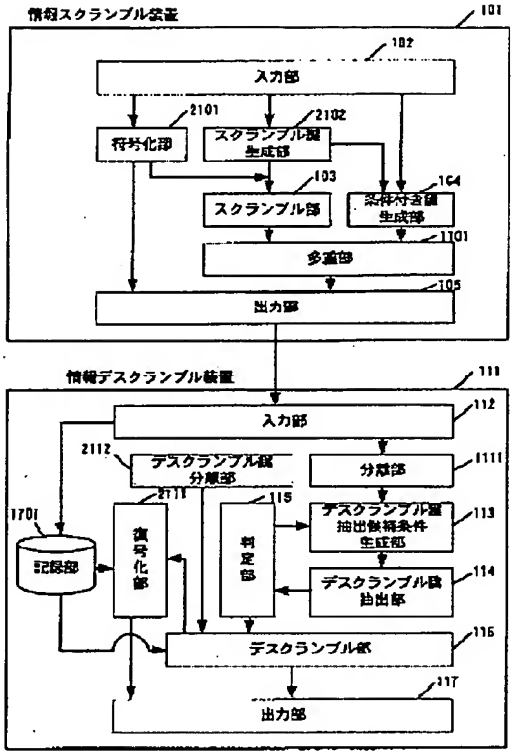
【図２５】



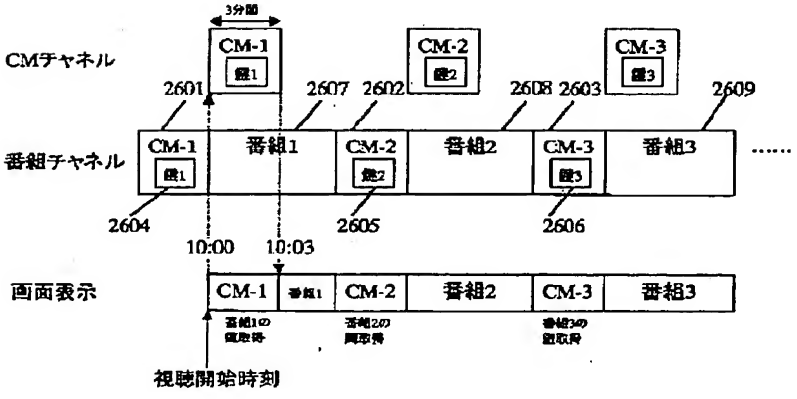
【図１９】



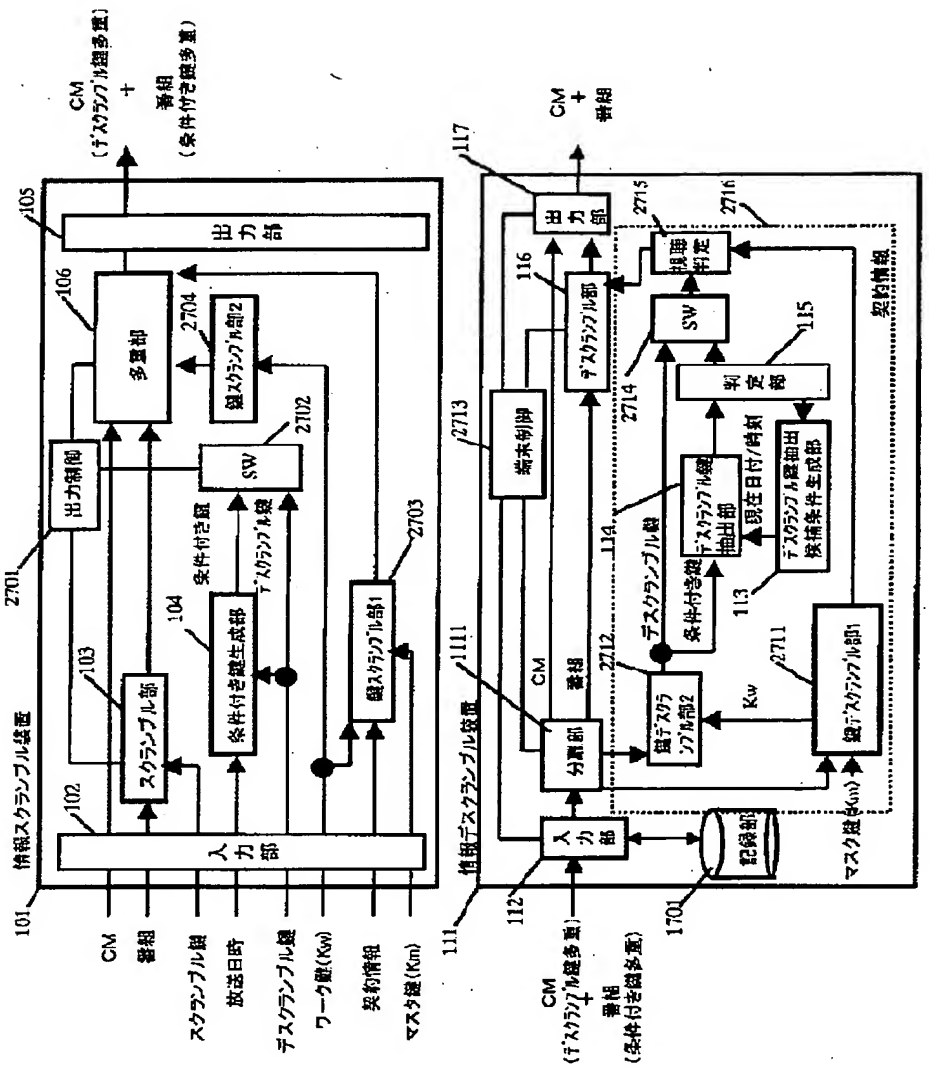
【図２１】



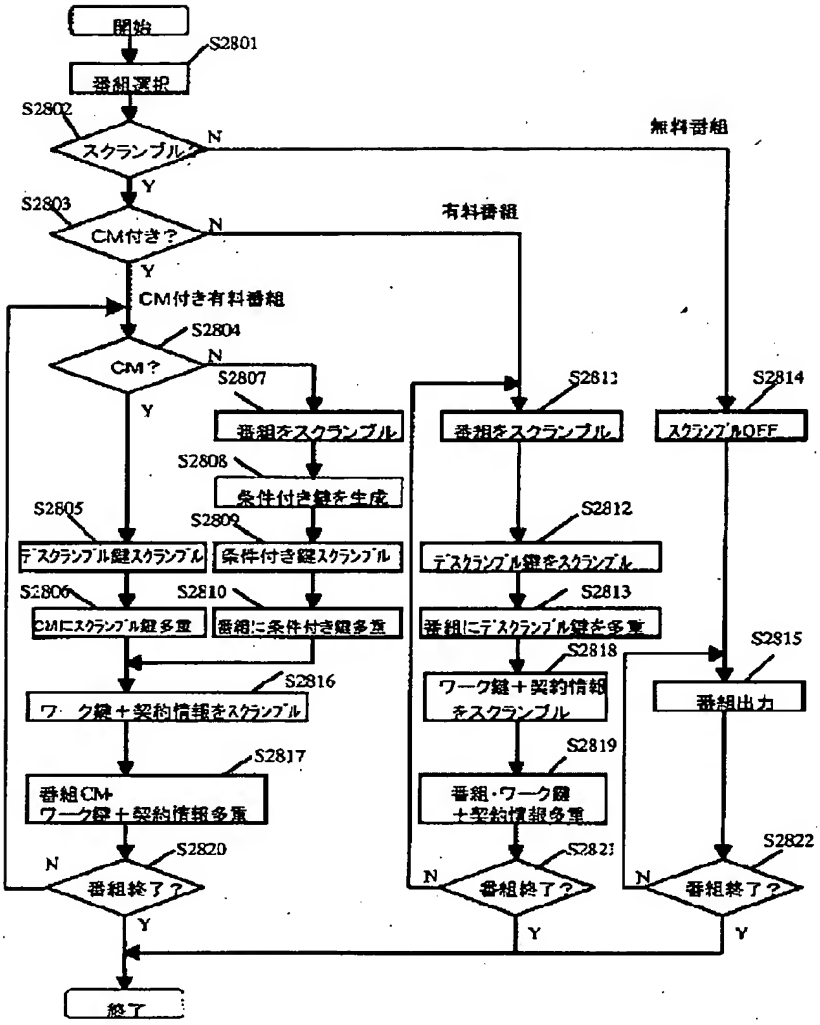
【図２６】



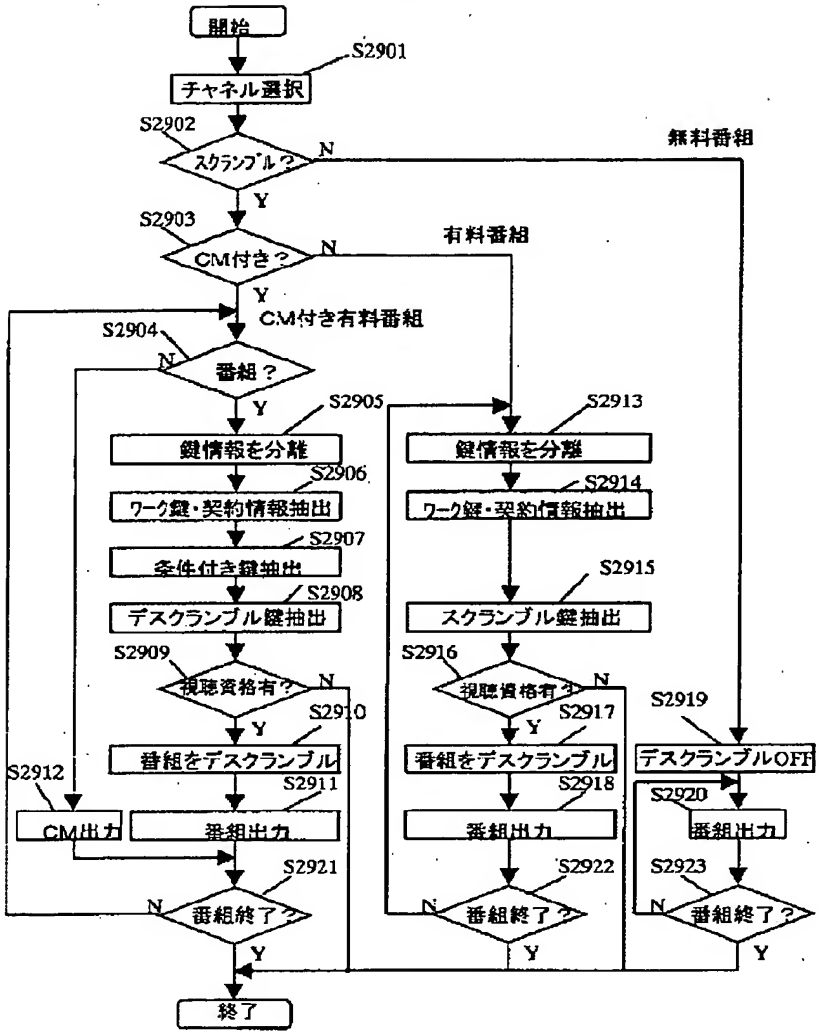
【図２７】



【図２８】



【図２９】



【図３０】